Overgroups of a linear Singer cycle in classical groups

by

Tom Brookfield

A thesis submitted to
The University of Birmingham
for the degree of
Doctor of Philosophy

School of Mathematics
The University of Birmingham
September 2014

UNIVERSITY OF
BIRMINGHAM

University of Birmingham Research Archive

e-theses repository

This unpublished thesis/dissertation is copyright of the author and/or third parties. The intellectual property rights of the author or third parties in respect of this work are as defined by The Copyright Designs and Patents Act 1988 or as modified by any successor legislation.

Any use made of information contained in this thesis/dissertation must be in accordance with that legislation and must be properly acknowledged. Further distribution or reproduction in any format is prohibited without the permission of the copyright holder.

Abstract

There are well known embeddings of $\mathrm{GL}_n(q)$ in $\mathrm{Sp}_{2n}(q)$ and $\mathrm{GO}_{2n}^{+}(q)$, as well as an embedding of $\mathrm{GL}_n(q^2)$ in $\mathrm{GU}_{2n}(q)$. These give embeddings of Singer cycles of $\mathrm{GL}_n(q)$ and $\mathrm{GL}_n(q^2)$ in the corresponding classical group, which we call *linear Singer cycles*. In this thesis, we classify the overgroups of such a Singer cycle in these groups.

Acknowledgements

First I would like to thank my supervisor, Professor Chris Parker for his time, support, guidance and patience. I would also like to thank the postgraduate students of the University of Birmingham, School of Mathematics for making the whole experience bearable. I also thank my family for their support and encouragement throughout my time at university. Finally, I gratefully acknowledge the financial support I have received from the EPSRC.

Contents

Chapter 1

Introduction

A Singer cycle of $\mathrm{GL}_n(q)$ is an element of order $q^n - 1$. These were shown to exist in [30] as a result of the fact that the multiplicative group of the field $\mathrm{GF}(q^n)$ is cyclic. We can also define Singer cycles in other classical groups as shown in [19]. If a classical group contains an irreducible cyclic subgroup, we can define a Singer cycle to be the generator of an irreducible cyclic subgroup of maximum possible order.

The presence of a Singer cycle in a group can tell you something about its structure. For instance, a result of Kantor [21] says that a subgroup of $\mathrm{GL}_n(q)$ that contains a Singer cycle normalizes a subgroup isomorphic to $\mathrm{GL}_{n/s}(q^s)$, for some s dividing n. There are also results by Bereczky [4], Malle et al [27] and Seitz [29] which classify the subgroups of other classical groups containing a Singer cycle of its corresponding classical group.

Let X be one of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}^+_{2n}(q)$ and let

$$u := \begin{cases} 2, & \text{if } X = \mathrm{GU}_{2n}(q), \\ 1, & \text{otherwise.} \end{cases}$$

There are well known embeddings of $\mathrm{GL}_n(q^u)$ in X, which give rise to embeddings of Singer cycles of $\mathrm{GL}_n(q^u)$ in X, which we call *linear Singer cycles* as in [8]. In this thesis, we classify the subgroups of X that contain a linear Singer cycle of X. When

$n = 1$, we compute all overgroups of a linear Singer cycle by a straightforward application of Dickson's [11] classification of the subgroups of $\mathrm{PSL}_2(q)$. When $n \geqslant 2$, we give a collection of subgroups such that any overgroup of a linear Singer cycle of X is contained in one of these subgroups. In Chapter 7, we explain how we can determine all overgroups of a linear Singer cycle of X.

In Chapter 2, we collect some preliminary definitions and results which we shall use throughout this thesis. This includes background information on Singer cycles, primitive prime divisors and bilinear and sesquilinear forms. Our main tool in the proof of the main theorems is a theorem of Aschbacher [2]. This states that a subgroup of a classical group either lies in one of eight geometrically defined classes or lies in a collection of subgroups which are almost simple modulo scalars. In this chapter, we also present a version of this theorem for $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ and $\mathrm{GO}^+_{2n}(q)$ and give the structure of the maximal members of the geometric classes.

In Chapter 3, we give the precise embeddings of $\mathrm{GL}_n(q^u)$ in X and use this to define the linear Singer cycles of X. We then give the actions of these on the underlying vector space and give some properties of these actions. The highlight of this chapter is the computation of all invariant subspaces of a linear Singer cycle. In most cases, the only proper non-trivial invariant subspaces are the subspaces W_1 and W_2, which we will define in this chapter. However when n and q are small, there are some other exceptional invariant subspaces. We conclude this chapter by applying our classification of invariant subspaces to the computation of the centralizer and normalizer of a linear Singer cycle in X.

In Chapter 4, we give the main theorems of this thesis. These can be stated as follows.

Theorem 1.0.1 *Let $G \leqslant \mathrm{Sp}_{2n}(q)$ with $n \geqslant 4$ and suppose that G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. Then G is contained in one of the following:*

1. $\mathrm{Stab}_{\mathrm{Sp}_{2n}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{Sp}_{2n}(q)}(W_2)$. *Both groups have the structure* $q^{n(n+1)/2} : \mathrm{GL}_n(q)$*;*

2. $\mathrm{GL}_n(q).2$, *with q odd;*

3. $\mathrm{Sp}_{2n/s}(q^s).s$, *where s is a prime dividing n;*

4. $\mathrm{GU}_n(q).2$, *with n even and q odd; or*

5. $\mathrm{GO}_{2n}^{+}(q)$, *with q even.*

Theorem 1.0.2 *Let $G \leqslant \mathrm{GU}_{2n}(q)$ with $n \geqslant 3$ and suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Then G is contained in one of the following:*

1. $\mathrm{Stab}_{\mathrm{GU}_{2n}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{GU}_{2n}(q)}(W_2)$. *Both groups have the structure $q^{n^2} : \mathrm{GL}_n(q^2)$;*

2. $\mathrm{GL}_n(q^2).2$; *or*

3. $\mathrm{GU}_{2n/s}(q^s).s$, *where s is an odd prime.*

Theorem 1.0.3 *Let $n \geqslant 5$ and let G be a subgroup of $\mathrm{GO}_{2n}^{+}(q)$ not containing $\Omega_{2n}^{+}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$. Then G is contained in one of the following:*

1. $\mathrm{Stab}_{\mathrm{GO}_{2n}^{+}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{GO}_{2n}^{+}(q)}(W_2)$. *Both groups have the structure $q^{n(n-1)/2} : \mathrm{GL}_n(q)$;*

2. $\mathrm{GL}_n(q).2$;

3. $\mathrm{GO}_{2n/s}^{+}(q^s).s$, *where s is a prime dividing n; or*

4. $\mathrm{GU}_n(q).2$, *with n even.*

In lower dimensions, the same properties hold. However, there are also some exceptional examples that occur when q is small. For example, when $X = \mathrm{Sp}_4(3)$, the linear Singer cycle is contained in a Sylow 2-subgroup of a group isomorphic to $2_{-}^{1+4}.\Omega_4^{-}(2)$. In this chapter, we also deal with the case when $n = 1$. As the subgroup lists for $\mathrm{GO}_{2n}^{+}(q)$

in [24, §4] and [36, Theorem 3.12] only apply when $n \geqslant 3$, we also deal with the case when $X = \mathrm{GO}_4^+(q)$. Since $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$, we apply a result on the maximal subgroups of direct products of simple groups in this case.

In Chapter 5, we begin the proof of the main theorems by considering the geometric classes of Aschbacher's Theorem. It is in these classes that the main examples of overgroups occur. We mainly use primitive prime divisors and bounds on the element orders of classical groups to deal with these examples.

Chapter 6 consists of the second half of the proof of the main theorems. Here we deal with the collection of groups, G that satisfy

$$S \leqslant G/\left(G \cap \mathrm{Z}(X)\right) \leqslant \mathrm{Aut}(S),$$

where S is a non-abelian simple group. We therefore apply the classification of finite simple groups, which states that a non-abelian simple group is either a sporadic group, a simple group of Lie-type or an alternating group on at least 5 letters. We therefore break this chapter into four parts. First we assume that S is one of the 26 sporadic simple groups. These cases can be dealt with by by considering the maximum element orders and the minimum projective representation degrees of such groups. We then assume S is an alternating group, where we use primitive prime divisors and a theorem of Feit [13]. Finally, we apply a similar method to [15, Proposition 7.2, Proposition 8.1] to the case when S is a simple group of Lie-type. Since, we use bounds on the minimum projective representation degrees of such groups, we distinguish between the cases when the Lie-type group is defined over a field of characteristic dividing q and when the characteristic is coprime to q.

Throughout this thesis, q is a power of a prime p, all groups are finite and all vector spaces are finite dimensional. We use Atlas [9] notation for groups and group extensions.

Chapter 2

Preliminaries

In this chapter, we give some preliminary definitions and results which we will use throughout this thesis.

2.1 Singer cycles

Definition 2.1.1 A *Singer cycle* of $\mathrm{GL}_n(q)$ is an element of order $q^n - 1$. We call the subgroup generated by a Singer cycle a *Singer subgroup.*

Lemma 2.1.2 *If q is a power of a prime, then $\mathrm{GL}_n(q)$ contains Singer cycles for all n and q.*

Proof. Let V be the underlying vector space of $\mathrm{GL}_n(q)$ and let λ be a generator for the multiplicative group of the finite field $\mathrm{GF}(q^n)$. Then identifying V with $\mathrm{GF}(q^n)$, we see that left multiplication by λ determines a bijective linear map from V to itself and this map has order $q^n - 1$. □

When we refer to a Singer cycle of $\mathrm{GL}_n(q)$, we will refer to the Singer cycle given in Lemma 2.1.2. That is, the map $a_\lambda : V \to V$ defined by

$$va_\lambda = \lambda v,$$

where λ is a generator of $\mathrm{GF}(q^n)^\times$. The next result says we can do this.

Proposition 2.1.3 *[18, p.187] All Singer subgroups of* $\mathrm{GL}_n(q)$ *are conjugate.*

A useful property of Singer subgroups of $\mathrm{GL}_n(q)$ is that they act regularly on non-zero vectors of the underlying vector space V. To see this, we identify $V \setminus \{0\}$ with $\mathrm{GF}(q^n)^\times$ and then, given $x, y \in V \setminus \{0\}$, we see that $xa_{x^{-1}y} = y$ and $xa_\lambda = x$ if and only if $\lambda = 1$.

Also if $\mathfrak{A}$ is a Singer subgroup of $\mathrm{GL}_n(q)$ and W is a non-zero $\mathfrak{A}$-invariant subspace of V, then for any $v \in W \setminus \{o\}$, the vectors

$$0,\ \lambda v,\ \lambda^2 v,\ \ldots,\ \lambda^{q^n-1} v$$

lie in W. Since the Singer cycle acts regularly on $V \setminus \{0\}$, these vectors are all distinct and so

$$q^n \leqslant |W| \leqslant |V| = q^n$$

and $W = V$. This says that $\mathfrak{A}$ acts irreducibly on V.

It can also be shown that Singer cycles in $\mathrm{GL}_n(q)$ are the elements of maximal order in $\mathrm{GL}_n(q)$, see for example [28, Proposition 3.27].

Singer cycles are useful as they can determine the structure of a group, as shown by a theorem of Kantor.

Theorem 2.1.4 *[21] If* $G \leqslant \mathrm{GL}_n(q)$ *contains a Singer cycle, then* $\mathrm{GL}_{n/s}(q^s) \trianglelefteq G$*, for some* s *dividing* n*.*

The subgroups $\mathrm{GL}_{n/s}(q^s)$ arise as follows: if V' is an n/s-dimensional vector space over $\mathrm{GF}(q^s)$, then we can view V' as an n-dimensional vector space, V over $\mathrm{GF}(q)$. When we do this, an invertible $\mathrm{GF}(q^s)$-linear transformation of V' can be viewed as an invertible

$\mathrm{GF}(q)$-linear transformation of V. Therefore, we get the following embedding:

$$\mathrm{GL}_{n/s}(q^s) \cong \mathrm{GL}(V') \leqslant \mathrm{GL}(V) \cong \mathrm{GL}_n(q).$$

Note that these subgroups do indeed contain Singer cycles since the Singer cycle of $\mathrm{GL}_{n/s}(q^s)$ has order $(q^s)^{n/s} - 1 = q^n - 1$, and is contained in $\mathrm{GL}_n(q)$. Since all cyclic subgroups of order $q^n - 1$ in $\mathrm{GL}_n(q)$ are conjugate, the Singer subgroup of $\mathrm{GL}_n(q)$ is contained in a conjugate of $\mathrm{GL}_{n/s}(q^s)$.

Moreover, if we take $s = n$, then we get the subgroup $\mathrm{GL}_1(q^n)$ of $\mathrm{GL}_n(q)$, which we can view as the Singer subgroup.

It is useful to know the structure of the centralizer and normalizer of a Singer subgroup in $\mathrm{GL}_n(q)$. A result of Huppert gives this.

Lemma 2.1.5 *[18, p.187] If $\mathfrak{A}$ is the Singer subgroup of $\mathrm{GL}_n(q)$, then $\mathrm{C}_{\mathrm{GL}_n(q)}(\mathfrak{A}) = \mathfrak{A}$ and $\mathrm{N}_{\mathrm{GL}_n(q)}(\mathfrak{A})/\mathfrak{A}$ is cyclic of order n.*

We will explicitly construct the normalizer of the Singer subgroup of $\mathrm{GL}_n(q)$. But to do this, we will need to discuss semilinear transformations.

Let F be a field and E a subfield. If V is an F-vector space, then a *semilinear transformation of V* is function $\gamma : V \longrightarrow V$ that satisfies for all $\lambda \in F$ and $v, w \in V$,

$$\begin{aligned} (v+w)\gamma &= v\gamma + w\gamma \\ (\lambda v)\gamma &= \lambda^\sigma v\gamma, \end{aligned}$$

where σ is a field automorphism of F lying in $\mathrm{Gal}(F/E)$, called the *companion automorphism of γ*. The group of invertible semilinear transformations of an n-dimensional F-vector space with companion automorphisms lying in $\mathrm{Gal}(F/E)$ is denoted $\Gamma\mathrm{L}_n(F/E)$ and is called the *general semilinear group*. If F and E are finite fields of sizes x and y, respectively, then we write $\Gamma\mathrm{L}_n(x/y)$ for $\Gamma\mathrm{L}_n(F/E)$ and $\mathrm{Gal}(x/y)$ for $\mathrm{Gal}(F/E)$. Also, if E is the prime subfield of F, then we just write $\Gamma\mathrm{L}_n(F)$, instead of $\Gamma\mathrm{L}_n(F/E)$.

Now there is a surjective group homomorphism from $\Gamma\mathrm{L}_n(F/E)$ to $\mathrm{Gal}(F/E)$, sending an element to its companion automorphism. This has kernel $\mathrm{GL}_n(F)$ and so

$$\Gamma\mathrm{L}_n(F/E)/\mathrm{GL}_n(F) \cong \mathrm{Gal}(F/E).$$

Moreover, we can view $\mathrm{Gal}(F/E)$ as a subgroup of $\Gamma\mathrm{L}_n(F/E)$ by identifying it with $\{I\sigma : \sigma \in \mathrm{Gal}(F/E)\}$, and it can be shown that

$$\Gamma\mathrm{L}_n(F/E) \cong \mathrm{GL}_n(F) : \mathrm{Gal}(F/E).$$

We are now in a position to describe the normalizer of the Singer subgroup of $\mathrm{GL}_n(q)$.

Proposition 2.1.6 *If* $\mathfrak{A}$ *is the Singer subgroup of* $\mathrm{GL}_n(q)$, *then* $\mathrm{N}_{\mathrm{GL}_n(q)}(\mathfrak{A}) = \Gamma\mathrm{L}_1(q^n/q)$.

Proof. We first show that $\Gamma\mathrm{L}_1(q^n/q)$ is a subgroup of $\mathrm{GL}_n(q)$. Define the map sending $\gamma \in \Gamma\mathrm{L}_1(q^n/q)$ to itself. We can view γ as a $\mathrm{GF}(q)$-semilinear transformation of an n-dimensional vector space. But, letting $\sigma \in \mathrm{Gal}(q^n/q)$ be the companion automorphism of γ, we have for all $\lambda \in \mathrm{GF}(q)$ and $v, w \in V$:

$$(v + \lambda w)\gamma = v\gamma + \lambda^\sigma w\gamma = v\gamma + \lambda w\gamma,$$

so in fact the image of γ is $\mathrm{GF}(q)$-linear, so lies in $\mathrm{GL}_n(q)$. The map is clearly an injective group homomorphism, so $\Gamma L_1(q^n/q)$ is isomorphic to a subgroup of $\mathrm{GL}_n(q)$.

Now, we know that $\mathrm{GL}_1(q^n) \trianglelefteq \Gamma\mathrm{L}_1(q^n/q)$ and $\Gamma\mathrm{L}_1(q^n/q) \leqslant \mathrm{GL}_n(q)$ so $\Gamma\mathrm{L}_1(q^n/q) \leqslant \mathrm{N}_{\mathrm{GL}_n(q)}(\mathfrak{A})$. But by Lemma 2.1.5, we have

$$|\Gamma\mathrm{L}_1(q^n/q)| / |\mathrm{GL}_1(q^n)| = n = \left|\mathrm{N}_{\mathrm{GL}_n(q)}(\mathfrak{A})\right| / |\mathfrak{A}|,$$

so $\mathrm{N}_{\mathrm{GL}_n(q)}(\mathfrak{A}) = \Gamma\mathrm{L}_1(q^n/q)$. □

From [19], we can also define Singer subgroups in other classical groups. They are defined as irreducible cyclic subgroups of maximal possible orders and are the intersection of the classical groups with the Singer subgroup of $\mathrm{GL}_n(q)$.

The following theorem of Bereczky gives conditions on a maximal overgroup of a Singer subgroup of one of these classical groups. Here d is odd, when $X = \mathrm{GU}_d(q)$ or $\mathrm{SU}_d(q)$ and d is odd, when $X = \mathrm{Sp}_d(q)$, $\mathrm{GO}_d^-(q)$, $\mathrm{SO}_d^-(q)$ or $\Omega_d^-(q)$. The odd-dimensional unitary groups and the plus type orthogonal groups are not dealt with as these classical groups do not contain irreducible cyclic subgroups.

Theorem 2.1.7 (Bereczky) *[4] Let X be one of $\mathrm{SL}_d(q)$, $\mathrm{GU}_d(q)$, $\mathrm{SU}_d(q)$, $\mathrm{Sp}_d(q)$, $\mathrm{GO}_d^-(q)$, $\mathrm{SO}_d^-(q)$ or $\Omega_d^-(q)$, where $d \geqslant 2$. Also let $H < X$ be a maximal overgroup of a Singer subgroup of X. Then one of the following holds:*

1. *H is an extension field type subgroup of X;*
2. *$X = \mathrm{SL}_d(q)$ and $(d,q) = (2,2), (2,5), (2,7), (2,9)$ or $(3,4)$;*
3. *$X = \mathrm{GU}_d(q)$ and $(d,q) = (3,2), (3,3)$ or $(5,2)$;*
4. *$X = \mathrm{SU}_d(q)$ and $(d,q) = (3,2), (3,3), (3,5)$ or $(5,2)$;*
5. *$X = \mathrm{Sp}_d(q)$ with q even and $\Omega_d^-(q) < H$;*
6. *$X = \mathrm{Sp}_d(q)$ and $(d,q) = (2,2), (2,5), (2,7), (2,9), (4,3)$ or $(8,2)$;*
7. *$X = \mathrm{GO}_d^-(q)$ with q odd and $H = \mathrm{SO}_d^-(q)$;*
8. *$X = \mathrm{GO}_d^-(q) = \mathrm{SO}_d^-(q)$ with q even and $H = \Omega_d^-(q)$;*
9. *$X = \mathrm{GO}_d^-(q)$ and $(d,q) = (4,3)$ or $(6,2)$;*
10. *$X = \mathrm{SO}_d^-(q)$ or $\Omega_d^-(q)$ and $(d,q) = (4,3), (6,2)$ or $(6,3)$.*

It can also be shown that each Singer subgroup contains the centre of the corresponding classical group, so we can view the Singer subgroups modulo the centre as Singer subgroups of the corresponding projective group.

2.2 Primitive prime divisors and bounds on the element order

A useful tool we will use in the proof of the main theorem is the notion of a primitive prime divisor.

Definition 2.2.1 If a and m are positive integers greater than 1, then a prime r dividing $a^m - 1$ is said to be a *primitive prime divisor* of $a^m - 1$ if it does not divide $a^i - 1$ for any i with $1 \leqslant i < m$.

The following theorem gives a criterion for the existence of a primitive prime divisor.

Theorem 2.2.2 (Zsigmondy) *[37] If a and m are positive integers greater than 1, then primitive prime divisors of $a^m - 1$ exist, unless $(a, m) = (2, 6)$ or $m = 2$ and $a + 1$ is a power of 2.*

Remarks 2.2.3 *1.* If r is a primitive prime divisor of $a^m - 1$, then a has order m modulo r. By Fermat's Little Theorem, we also have $a^{r-1} \equiv 1 \pmod{r}$, which means $r - 1 = xm \geqslant m$ for some $x \in \mathbb{N}$. If $m \geqslant 2$, this means that r is odd.

2. If r divides $a^{sm+t} - 1$, with $0 \leqslant t < m$, then r divides

$$\left(a^{sm+t} - 1\right) - \left(a^{sm} - 1\right) = a^{sm}\left(a^t - 1\right).$$

Since $a^m - 1$ and a are coprime, r must divide $q^t - 1$, which forces $t = 0$. Hence, if r is a primitive prime divisor of $a^k - 1$, then m divides k.

If a given group contained a Singer cycle, then its order would have to be divisible by a primitive prime divisor of $q^n - 1$, if one exists. We will use this fact to rule out many of the possibilities for overgroups in the proof of the main theorems. When we assume that a primitive prime divisor of $q^n - 1$ does not exist, we will often assume either $n = 2$ or $(n, q) = (6, 2)$.

At one point in Chapter 6, we will use the notion of a large primitive prime divisor.

Definition 2.2.4 If a and m are positive integers greater than 1, then a primitive prime divisor r of $a^m - 1$ is called *large* if either $r > m + 1$ or r^2 divides $a^m - 1$. A primitive prime divisor is called *small* if it is not large.

The following gives the conditions on a and m for which a large primitive prime divisor of $a^m - 1$ exists.

Theorem 2.2.5 *[13] If a and m are integers greater than 1, then there exists a large primitive prime divisor of $a^m - 1$ except in the following cases.*

i) $m = 2$ *and* $a = 2^s 3^t - 1$, *for some natural number* s, *and* $t = 0$ *or* 1.

ii) $a = 2$ *and* $m = 4, 6, 10, 12$ *or* 18.

iii) $a = 3$ *and* $m = 4$ *or* 6.

iv) $(a, m) = (5, 6)$.

In addition to primitive prime divisors, we shall frequently make use of bounds on the maximum element orders of classical groups. These are particularly useful in Chapter 6, where a Singer cycle is contained in the automorphism group of a simple group of Lie-type. We shall also make use of MAGMA [5] and the ATLAS [9] for the maximum element orders of other simple groups.

Theorem 2.2.6 *[14, Theorem 2.6] The maximum element orders of the automorphism groups of the the classical simple groups are shown in Table 2.1.*

Simple Group T	Maximum element order in $\mathrm{Aut}(T)$	Remarks
$\mathrm{PSL}_n(q)$	$(q^n-1)/(q-1)$	$(n,q)\neq(2,4),(3,2)$
	6	$(n,q)=(2,4)$
	8	$(n,q)=(3,2)$
$\mathrm{PSp}_{2n}(q)$	$\leqslant q^{n+1}/(q-1)$	$(n,q)\neq(2,2)$
$\mathrm{Sp}_4(2)$	10	$(n,q)=(2,2)$
$\mathrm{PSU}_n(q)$	$q^{n-1}-1$	n odd, $q>p$ and $(n,q)\neq(3,4)$
	16	$(n,q)=(3,4)$
	$(p^{n-2}+1)\,q$	n odd, $q=p$ and $(n,q)\neq(5,2)$
	24	$(n,q)=(5,2)$
	$q^{n-1}+1$	n even and $q>2$
	$4\,(2^{n-3}+1)$	n even and $q=2$
$\mathrm{P}\Omega_{2n+1}(q)$	$\leqslant q^{n+1}/(q-1)$	
$\mathrm{P}\Omega^{+}_{2n}(q)$	$\leqslant q^{n+1}/(q-1)$	
$\mathrm{P}\Omega^{-}_{2n}(q)$	$\leqslant q^{n+1}/(q-1)$	

Table 2.1: Maximum element order in automorphism groups of classical simple groups

2.3 Bilinear and sesquilinear forms

Here, we collect information on bilinear and sesquilinear forms on vector spaces which we shall use in Chapter 3. More information can be found in [3, §7] and [24, §2.1].

A *bilinear form* on a vector space V over a field F is a function $f : V \times V \to F$ that satisfies

$$f(\lambda u + \mu v, w) = \lambda f(u, w) + \mu f(v, w)$$

and

$$f(u, \lambda v + \mu w) = \lambda f(u, v) + \mu f(u, w),$$

for all $u, v, w \in V$ and $\lambda, \mu \in F$. It is *symmetric* if $f(u, v) = f(v, u)$, for all $u, v \in F$; *skew-symmetric* if $f(u, v) = -f(v, u)$, for all $u, v \in F$; and *alternating* if $f(v, v) = 0$ for all $v \in F$.

Note that if f is alternating, then it is skew symmetric. Conversely, if F has odd characteristic and if f is skew symmetric, then f is alternating. However if F has characteristic two, then f can be skew symmetric but not alternating.

A *conjugate symmetric sesquilinear form* on V over a field F that has an automorphism σ of order 2, is a function $f : V \times V \to F$ that satisfies

$$f(\lambda u + \mu v, w) = \lambda f(u, w) + \mu f(v, w)$$

and $f(u, v) = f(v, u)^{\sigma}$, for all $u, v, w \in V$ and $\lambda, \mu \in F$.

If $X \subseteq V$, then define the subspace

$$X^{\perp} = \{v \in V : f(x, v) = 0, \text{ for all } x \in X\}.$$

The set $V^{\perp}$ is called the radical of f and is denoted $\mathrm{Rad}(f)$. We say that f is non-degenerate if $\mathrm{Rad}(f) = \{0\}$.

A non-degenerate, skew symmetric, alternating bilinear form is called a *symplectic form.* A non-degenerate conjugate symmetric sesquilinear form is called a *unitary form.* A non-degenerate symmetric bilinear form that is alternating in characteristic 2 is called an *orthogonal form.*

A vector $v \in V$ is called *isotropic* if $f(v,v) = 0$. A subspace W of V is called *totally isotropic* if f restricted to W is zero. We say that W is *non-degenerate* if f restricted to W is non-degenerate.

A *quadratic form* on V over F is a function $Q : V \to F$ such that $Q(\lambda v) = \lambda^2 Q(v)$ for all $v \in V$, $\lambda \in F$ and the function $f_Q : V \times V \to F$ defined by

$$f_Q(u,v) = Q(u+v) - Q(u) - Q(v)$$

is a symmetric bilinear form. A quadratic form Q is *non-degenerate* if f_Q is non-degenerate.

A vector space together with a symplectic form is called a *symplectic space.* A vector space together with a unitary form is called a *unitary space.* A vector space together with a quadratic form and an associated bilinear form is called an *orthogonal space.*

If V is an orthogonal space, a vector $v \in V$ is called *singular* if v is isotropic and $Q(v) = 0$. If v is a singular vector, then it is also isotropic. Conversely, if F has odd characteristic and v is isotropic, then v is singular. But if F has characteristic two, then every vector is isotropic, but not all vectors are singular.

A subspace W of V is called *totally singular* if W is totally isotropic and every vector of W is singular. The *Witt index* of V is the maximum dimension of a totally singular subspace.

If V is a symplectic, unitary or orthogonal space with form f, then an *isometry* g of V is an invertible linear transformation of V that satisfies $f(ug, vg) = f(u,v)$ for all

$u, v \in V$.

The group of isometries of a $2n$-dimensional symplectic space over $\mathrm{GF}(q)$ is called the *symplectic group* and is denoted $\mathrm{Sp}_{2n}(q)$. The group of isometries of an n-dimensional unitary space over $\mathrm{GF}(q^2)$ is called the *general unitary group*, denoted by $\mathrm{GU}_n(q)$. If n is odd then the group of isometries of an n-dimensional orthogonal space is denoted by $\mathrm{GO}_n(q)$. If n is even, then the group of isometries of an n-dimensional orthogonal space with Witt index $n/2-1$ is denoted by $\mathrm{GO}_n^-(q)$ and we say the quadratic form has *minus type*. The group of isometries of an n-dimensional orthogonal space with Witt index $n/2$ is denoted by $\mathrm{GO}_n^+(q)$ and we say the quadratic form has *plus type*. These groups are *called the orthogonal groups.*

In this thesis, we shall be concerned with the groups $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ and $\mathrm{GO}_{2n}^+(q)$. We shall need the following fact to define linear Singer cycles of these groups.

Proposition 2.3.1

1. *[24, Proposition 2.4.1] Let V be a $2n$-dimensional symplectic vector space with symplectic form f_S. Then there is a basis $v_1, \ldots, v_n, w_1, \ldots w_n$ of V such that for all i, j, we have $f_S(v_i, v_j) = f_S(w_i, w_j) = 0$ and $f_S(v_i, w_j) = \delta_{ij}$.*

2. *[24, Proposition 2.3.2] Let V be a $2n$-dimensional unitary vector space with unitary form f_U. Then there is a basis $v_1, \ldots, v_n, w_1, \ldots w_n$ of V such that for all i, j, we have $f_U(v_i, v_j) = f_U(w_i, w_j) = 0$ and $f_U(v_i, w_j) = \delta_{ij}$.*

3. *[24, Proposition 2.5.3] Let V be a $2n$-dimensional orthogonal vector space with quadratic form Q of plus type. Also, let f_Q be the symmetric bilinear form associated to Q. Then there is a basis $v_1, \ldots, v_n, w_1, \ldots w_n$ of V such that for all i, j, we have $Q(v_i) = Q(w_i) = 0$ and $f_Q(v_i, w_j) = \delta_{ij}$.*

We end this section with an important result on isometries of subspaces.

Lemma 2.3.2 (Witts Lemma) *Let V be a symplectic, unitary or orthogonal space and U a subspace. If $g : U \to U$ is an isometry, then we can extend g to an isometry of V.*

2.4 Maximal subgroups and Aschbacher's theorem

We require some results on subgroups of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ and $\mathrm{GO}^{+}_{2n}(q)$ in our analysis. When we deal with $\mathrm{Sp}_2(q)$ and $\mathrm{GU}_2(q)$, we will use a theorem of Dickson [11, §12] which gives the maximal subgroups of $\mathrm{PSL}_2(q)$. We have taken the result from [23, Corollary 2.2] and [31, Theorem 6.25].

Theorem 2.4.1 *Let $q \geqslant 4$ and $d = \gcd(2, q-1)$. If M is a maximal subgroup of $\mathrm{PSL}_2(q)$, then M is one of the following:*

1. $\mathrm{D}_{2(q-1)/d}$, *where $q \geqslant 13$ when q is odd;*

2. $\mathrm{D}_{2(q+1)/d}$, *where $q \neq 7$ or 9 when q is odd;*

3. *The semi-direct product of an elementary abelian group of order q with a cyclic group of order $(q-1)/d$;*

4. $\mathrm{PSL}_2(q_0)$, *where $q = q_0^m$ and m is prime, $m \neq 2$ when q is odd;*

5. $\mathrm{PGL}_2(q_0)$, *where q_0 is odd and $q = q_0^2$;*

6. A_4, *where q is a prime with $q \equiv \pm 3 \bmod 8$;*

7. S_4, *where $q \equiv \pm 1 \bmod 8$ and either q is prime or $q = p^2$ and $3 < p \equiv \pm 3 \bmod 8$;*

8. A_5, *where $q \equiv \pm 1 \bmod 10$ and either q is prime or $q = p^2$ and $p \equiv \pm 3 \bmod 10$.*

As a corollary, we can obtain the maximal subgroups of $\mathrm{PGL}_2(q)$.

Corollary 2.4.2 *[23, Corollary 2.3] If $q \geqslant 4$ and M is a maximal subgroup of $PGL_2(q)$, then M is one of the following:*

1. $\mathrm{D}_{2(q-1)}$, *for $q \neq 5$;*

2. $D_{2(q+1)}$;

3. *The semi-direct product of an elementary abelian group of order* q *with a cyclic group of order* $(q-1)$;

4. $PSL_2(q)$, *when* q *is odd;*

5. $PGL_2(q_0)$, *where* $q = q_0^m$ *and* m *is prime;*

6. S_4, *where* q *is a prime with* $q \equiv \pm 3 \bmod 8$.

For the majority of this thesis, we shall use a result of Aschbacher. This states that a subgroup of a given classical group either lies in one of eight geometrically defined classes or lies in a collection $\mathcal{S}$ of subgroups which are almost simple modulo scalars. We state a version of this theorem for the group X, where X is one of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}_{2n}^{+}(q)$. Before we do this, we collect some definitions needed to define $\mathcal{S}$ and give a brief description of the geometric classes.

The *socle* of a group is the product of its minimal normal subgroups. A group G is *perfect* if $G = G'$. A *central extension* of a group G is a group H together with a surjective homomorphism $\pi : H \to G$ such that $\mathrm{Ker}(\pi) \leqslant \mathrm{Z}(H)$. A central extension which is perfect is called a *covering group*. All covering groups of a perfect group are finite and every perfect group G has a unique covering group of maximal possible order, called the *full covering group of* G.

Let G be a group and V be an irreducible G-module over a field F. If E is an extension field of F, then we can form the tensor product $V \otimes E$, which is a G-module over E. We say that V is *absolutely irreducible* if $V \otimes E$ is irreducible for all extension fields E of F.

We can now define the collection $\mathcal{S}$.

Definition 2.4.3 *Let* X *be one of* $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ *or* $\mathrm{GO}_{2n}^{+}(q)$, *with* $n \geqslant 3$ *when* $X = \mathrm{GO}_{2n}^{+}(q)$ *and* $n \geqslant 2$ *otherwise. Let* X_0 *be one of* $\mathrm{Sp}_{2n}(q)$, $\mathrm{SU}_{2n}(q)$ *or* $\Omega_{2n}^{+}(q)$, *when X is $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}^{+}_{2n}(q)$, respectively. Also, let V be the vector space associated to X and*

$$u = \begin{cases} 2, & \text{if } X = \mathrm{GU}_{2n}(q), \\ 1, & \text{otherwise.} \end{cases}$$

A subgroup G of X not containing X_0 lies in $\mathcal{S}$ if and only if the following hold:

a) The socle of G is a non-abelian simple group, S, so that

$$S \leqslant G/\left(G \cap \mathrm{Z}(X)\right) \leqslant \mathrm{Aut}(\mathrm{S}).$$

b) If L is the full covering group of S and $\rho : L \to \mathrm{GL}_{2n}(q^u)$ is a representation of L corresponding to G, in the sense that $\rho(L) \leqslant G$ and

$$\rho(L) / \left(\rho(L) \cap \mathrm{Z}(X)\right) \cong S,$$

then $\rho(L)$ is absolutely irreducible.

c) $\rho(L)$ cannot be realized over a proper subfield of $\mathrm{GF}(q^u)$.

d) If $\rho(L)$ preserves a non-degenerate quadratic form on V, then $X_0 = \Omega^{+}_{2n}(q)$.

e) If $\rho(L)$ preserves a non-degenerate symplectic form but no non-degenerate quadratic form on V, then $X_0 = \mathrm{Sp}_{2n}(q)$.

f) If $\rho(L)$ preserves a non-degenerate unitary form on V, then $X_0 = \mathrm{SU}_{2n}(q)$.

We now give a brief description of the geometrically defined classes, $\mathcal{C}_1, \ldots, \mathcal{C}_8$ appearing in Aschbacher's Theorem. The members of class $\mathcal{C}_1$ stabilize subspaces of V. These subspaces are either totally singular or non-degenerate. These groups are also referred to as *reducible.*

The class $\mathcal{C}_2$ contains the stabilizers of direct sum decompositions $V = \bigoplus_{i=1}^{t} V_i$, where $\dim(V_i) = \dim(V_j)$ for all i and j. These decompositions consist of either totally singular or non-degenerate subspaces of V. These groups are also referred to as *imprimitive*.

Class $\mathcal{C}_3$ is the class of extension field type subgroups. If u is as in Definition 2.4.3, then these subgroups preserve an extension field of $\mathrm{GF}(q^u)$ of prime index.

The class $\mathcal{C}_4$ contains the stabilizers of tensor product decompositions of the form $V = V_1 \otimes V_2$, where $\dim(V_1) \neq \dim(V_2)$.

Class $\mathcal{C}_5$ is the class of subfield subgroups. As opposed to $\mathcal{C}_3$, these preserve a subfield of $\mathrm{GF}(q^u)$ of prime index.

Now, if r is a prime, then a *group of symplectic-type* is an r-group that satisfies

$$\Phi(R) = \mathrm{Z}(R) = R' = r$$

and every characteristic abelian subgroup of R is cyclic. Class $\mathcal{C}_6$ contains the normalizers of symplectic type r-groups lying in absolutely irreducible representations.

Class $\mathcal{C}_7$ contains the stabilizers of tensor product decompositions of the form $V = \bigotimes_{i=1}^{t} V_i$, where $\dim(V_i) = \dim(V_j)$ for all i and j. These groups are also referred to as *tensor induced*.

Finally, the class $\mathcal{C}_8$ contains classical subgroups. In our situation, these only occur when q is even and $X = \mathrm{Sp}_{2n}(q)$ and consist of the orthogonal groups $\mathrm{GO}_{2n}^{\pm}(q)$.

We are now in a position to state Aschbacher's Theorem for $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ and $\mathrm{GO}_{2n}^{+}(q)$.

Theorem 2.4.4 (Aschbacher) *[2] Let X be one of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}_{2n}^{+}(q)$, with $n \geqslant 3$ when $X = \mathrm{GO}_{2n}^{+}(q)$ and $n \geqslant 2$ otherwise. Let X_0 be one of $\mathrm{Sp}_{2n}(q)$, $\mathrm{SU}_{2n}(q)$ or $\Omega_{2n}^{+}(q)$, when X is $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}_{2n}^{+}(q)$, respectively. If G is a subgroup of X not containing X_0, then either G is contained in a member of $\mathcal{C}_1, \ldots, \mathcal{C}_8$ or G lies in $\mathcal{S}$.*

Class	Maximal member of class	Conditions
$\mathcal{C}_1$	$q^{k(4n-3k)} : \left(\mathrm{GL}_k\left(q^2\right) \times \mathrm{GU}_{2(n-k)}\left(q\right)\right)$	$1 \leqslant k \leqslant n$
	$\mathrm{GU}_k\left(q\right) \times \mathrm{GU}_{2n-k}\left(q\right)$	$1 \leqslant k < 2n$
$\mathcal{C}_2$	$\mathrm{GL}_n\left(q^2\right).2$	
	$\mathrm{GU}_k\left(q\right) \wr \mathrm{S}_m$	$2n = km$
$\mathcal{C}_3$	$\mathrm{GU}_{2n/s}\left(q^s\right).s$	s an odd prime
$\mathcal{C}_4$	$\mathrm{GU}_k\left(q\right) \circ \mathrm{GU}_m\left(q\right)$	$2n = km$
$\mathcal{C}_5$	$C_{q+1}.\mathrm{PGU}_{2n}\left(q_0\right)$	$q_0^m = q$, m an odd prime
	$C_{q+1} \circ \mathrm{GO}_{2n}^{\pm}\left(q\right)$	q odd
	$C_{q+1} \circ \mathrm{Sp}_{2n}\left(q\right)$	
$\mathcal{C}_6$	$C_{q+1} \circ 2^{1+2m}.\mathrm{Sp}_{2m}\left(2\right)$	$2n = 2^m$, $q \equiv 3 \bmod 4$
$\mathcal{C}_7$	$C_{q+1}.\left(\mathrm{PGU}_k\left(q\right) \wr \mathrm{S}_m\right)$	$2n = k^m$, $k \geqslant 3$

Table 2.2: Maximal members of the geometric classes in $\mathrm{GU}_{2n}\left(q\right)$.

In Tables 2.2, 2.3 and 2.4, we give the maximal members of the classes $\mathcal{C}_1, \ldots, \mathcal{C}_8$ in $\mathrm{Sp}_{2n}\left(q\right)$, $\mathrm{GU}_{2n}\left(q\right)$ and $\mathrm{GO}_{2n}^{+}\left(q\right)$, which we have taken from [6, §2.2], [24, §4] and [36, Theorems 3.7, 3.8, 3.9 and 3.12]. Note that in these tables, the notation $G\frac{1}{2}$ denotes a subgroup of index 2 in G, whereas the notation $\varepsilon = \circ$ in class $\mathcal{C}_4$ of Table 2.3 means m is odd and we write $\mathrm{GO}_m\left(q\right)$ instead of $\mathrm{GO}_m^{\circ}\left(q\right)$. We also do not write the $\pm$ signs in the subgroups $C_{q+1} \circ 2^{1+2m}.\mathrm{Sp}_{2m}\left(2\right)$ in class $\mathcal{C}_6$ of Table 2.2, as

$$C_{q+1} \circ 2_{+}^{1+2m} \cong C_{q+1} \circ 2_{-}^{1+2m}.$$

If G is a subgroup of $\mathrm{Sp}_{2n}\left(q\right)$, $\mathrm{GU}_{2n}\left(q\right)$ and $\mathrm{GO}_{2n}^{+}\left(q\right)$, lying in $\mathcal{C}_1, \ldots, \mathcal{C}_8$, then G is contained in one of the groups in these tables. We will use these in Chapter 5 when we consider which of these contain a linear Singer cycle.

Class	Maximal member of class	Conditions
$\mathcal{C}_1$	$q^{k\left(2n+\frac{1-3k}{2}\right)}:\left(\mathrm{GL}_k(q)\times\mathrm{Sp}_{2(n-k)}(q)\right)$	$1\leqslant k\leqslant n$
	$\mathrm{Sp}_{2k}(q)\times\mathrm{Sp}_{2(n-k)}(q)$	$1\leqslant k<n$
$\mathcal{C}_2$	$\mathrm{GL}_n(q).2$	q odd
	$\mathrm{Sp}_{2k}(q)\wr\mathrm{S}_m$	$n=km$
$\mathcal{C}_3$	$\mathrm{Sp}_{2n/s}(q^s).s$	s prime, $2n/s$ even
	$\mathrm{GU}_n(q).2$	q odd
$\mathcal{C}_4$	$(\mathrm{Sp}_{2k}(q)\circ\mathrm{GO}_m^{\varepsilon}(q)).\gcd(m,2)$	$n=km$, q odd, $m\geqslant 3$, $\varepsilon\in\{\circ,-,+\}$
$\mathcal{C}_5$	$\mathrm{Sp}_{2n}(q_0).\gcd(2,q-1,m)$	$q_0^m=q$, m prime
$\mathcal{C}_6$	$2_-^{1+2m}.\Omega_{2m}^-(2)$	$n=2^{m-1},\ q=p\geqslant 3,$ $p\equiv\pm 3\pmod 8$
	$2_-^{1+2m}.\mathrm{GO}_{2m}^-(2)$	$n=2^{m-1}$, $q=p\geqslant 3$, $p\equiv\pm 1\pmod 8$
$\mathcal{C}_7$	$2.(\mathrm{PSp}_{2k}(q).2\wr\mathrm{S}_m)\frac{1}{2}$	$2n=(2k)^m$, qm odd, $(k,q)\neq(2,3)$
$\mathcal{C}_8$	$\mathrm{GO}_{2n}^{\pm}(q)$	q even

Table 2.3: Maximal members of the geometric classes in $\mathrm{Sp}_{2n}(q)$.

Class	Maximal member in class	Conditions
$\mathcal{C}_1$	$q^{k\left(2n-\frac{1+3k}{2}\right)}:\left(\mathrm{GL}_k(q)\times \mathrm{GO}^+_{2(n-k)}(q)\right)$	$1\leqslant k\leqslant n,\ k\neq n-1$
	$\mathrm{GO}^{\varepsilon}_{2k}(q)\times \mathrm{GO}^{\varepsilon}_{2(n-k)}(q)$	$1\leqslant m<n$
	$\mathrm{GO}_{2k+1}(q)\times \mathrm{GO}_{2m+1}(q)$	q odd, $k+m+1=n$, either $k<m$
		or $k=m$ and $q\equiv 3 \bmod 4$
	$\mathrm{Sp}_{2n-2}(q)$	q even
$\mathcal{C}_2$	$\mathrm{GL}_n(q).2$	
	$\mathrm{GO}^+_{2k}(q)\wr \mathrm{S}_m$	$n=km$
	$\mathrm{GO}^-_{2k}(q)\wr \mathrm{S}_m$	$n=km$, m even
	$\mathrm{GO}_k(q)\wr \mathrm{S}_m$	$2n=km$, kq odd,
		n even or $q\equiv 1 \bmod 4$
$\mathcal{C}_3$	$\mathrm{GO}^+_{2n/s}(q^s).s$	s prime, $2n/s$ even
	$\mathrm{GU}_n(q).2$	n even
	$\mathrm{GO}_n(q^2).2$	nq odd
$\mathcal{C}_4$	$(\mathrm{Sp}_{2k}(q)\circ \mathrm{Sp}_{2m}(q)).\gcd(2,q-1)$	$n=2km$
	$\mathrm{GO}^+_{2k}(q)\times \mathrm{SO}_m(q)$	$n=km$, mq odd
	$(\mathrm{GO}^{\varepsilon_1}_{2k}(q)\circ \mathrm{GO}^{\varepsilon_2}_{2m}(q)).2$	$n=2km$, q odd, $m\geqslant 2$
$\mathcal{C}_5$	$\mathrm{GO}^+_{2n}(q_0)$	$q_0^m=q$, m prime
	$\mathrm{GO}^-_{2n}(q_0)$	$q_0^2=q$
$\mathcal{C}_6$	$2^{1+2m}_+.\Omega^+_{2m}(2)$	$n=2^{m-1}$, q prime,
		$q\equiv \pm 3 \pmod 8$
	$2^{1+2m}_+.\mathrm{GO}^+_{2m}(2)$	$n=2^{m-1}$, q prime,
		$q\equiv \pm 1 \pmod 8$
$\mathcal{C}_7$	$2.(\mathrm{PSp}_{2k}(q).2\wr \mathrm{S}_m)\frac{1}{2}$	$2n=(2k)^m$, qm even
	$2.\left(\mathrm{PGO}^{\pm}_{2k}(q).2\wr \mathrm{S}_m\right)\frac{1}{2}$	$2n=(2k)^m$, q odd,

Table 2.4: Maximal members of the geometric classes in $\mathrm{GO}^+_{2n}(q)$.

Chapter 3

Linear Singer cycles

Let X be one of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}_{2n}^{+}(q)$. In this chapter we define the linear Singer cycles of X, which are the subject of this thesis and determine how they act on the vector space, V associated to X.

3.1 Constructions

Throughout the rest of thesis, let

$$u = \begin{cases} 2, & \text{if } X = \mathrm{GU}_{2n}(q), \\ 1, & \text{otherwise.} \end{cases}$$

The following theorem shows that we can embed $\mathrm{GL}_n(q^u)$ in X. We follow the exposition in Huppert [18, §II. Satz 9.24] for the embedding of $\mathrm{GL}_n(q)$ in $\mathrm{Sp}_{2n}(q)$ and apply the argument to the unitary and orthogonal cases. Although the methods for each case are similar, we present each case individually to emphasize the precise embedding in each case.

Theorem 3.1.1 *1. There is an embedding of* $\mathrm{GL}_n(q)$ *in* $\mathrm{Sp}_{2n}(q)$*. Moreover, if* $g \in \mathrm{GL}_n(q)$ *and if* $\tilde{g}$ *is the matrix representing* g *with respect to some basis, then there* *is a basis of V such that g maps to the block matrix*

$$\left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-T} \end{array}\right).$$

2. *There is an embedding of $\mathrm{GL}_n\left(q^2\right)$ in $\mathrm{GU}_{2n}\left(q\right)$. Moreover, if $g \in \mathrm{GL}_n\left(q\right)$ and if $\tilde{g}$ is the matrix representing g with respect to some basis, then there is a basis of V such that g maps to the block matrix*

$$\left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-Tq} \end{array}\right).$$

3. *There is an embedding of $\mathrm{GL}_n\left(q\right)$ in $\mathrm{GO}^{+}_{2n}\left(q\right)$. Moreover, if $g \in \mathrm{GL}_n\left(q\right)$ and if $\tilde{g}$ is the matrix representing g with respect to some basis, then there is a basis of V such that g maps to the block matrix*

$$\left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-T} \end{array}\right).$$

Proof. 1. Let V be a $2n$-dimensional symplectic vector space over $\mathrm{GF}\left(q\right)$ with symplectic form f_S. By Proposition 2.3.1, V has a basis, $v_1, \ldots, v_n, w_1, \ldots, w_n$ such that $f_S\left(v_i, v_j\right) = f_S\left(w_i, w_j\right) = 0$ and $f_S\left(v_i, w_i\right) = \delta_{ij}$. Let g be a non-singular linear map on $\langle v_1, \ldots, v_n\rangle$ with $v_i g = \sum_{k=1}^{n} g_{ik} v_k$. Witt's Lemma says we can extend g to an isometry of V by setting $w_j h = \sum_{l=1}^{n} h_{jl} w_l$. For this, we need,

$$\begin{aligned} \delta_{ij} &= f_S\left(v_i, w_j\right) = f_S\left(v_i g, w_j h\right) = f_S\left(\sum_{k=1}^{n} g_{ik} v_k, \sum_{l=1}^{n} h_{jl} w_l\right) \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} g_{ik} h_{jl} f_S\left(v_k, w_l\right) = \sum_{k=1}^{n} g_{ik} h_{jk}. \end{aligned}$$

From this, we can conclude that $h = g^{-T}$. Therefore the map τ given by

$$g\tau = \left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-T} \end{array}\right)$$

is an isomorphism of $\mathrm{GL}_n(q)$ in $\mathrm{Sp}_{2n}(q)$.

2. Let V be a $2n$-dimensional unitary vector space over $\mathrm{GF}(q^2)$ with unitary form f_U. By Proposition 2.3.1, V has a basis $v_1, \ldots, v_n, w_1, \ldots, w_n$, such that $f_U(v_i, v_j) = f_U(w_i, w_j) = 0$ and $f_U(v_i, w_j) = \delta_{ij}$. Let g be an invertible linear map on $\langle v_1, \ldots, v_n \rangle$ with $v_i g = \sum_{k=1}^{n} g_{ik} v_k$. As before, we can use Witt's Lemma to extend g to an isometry of V by setting $w_j h = \sum_{l=1}^{n} h_{jl} w_l$. This time, letting $\sigma : x \mapsto x^q$ denote the field automorphism of $\mathrm{GF}(q^2)$ of order 2, we require

$$\begin{aligned} \delta_{ij} &= f_U(v_i, w_j) = f_U(v_i g, w_j h) = f_U\left(\sum_{k=1}^{n} g_{ik} v_k, \sum_{l=1}^{n} h_{jl} w_l\right) \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} g_{ik} h_{jl}^{\sigma} f_U(v_k, w_l) = \sum_{k=l}^{n} g_{ik} h_{jk}^{q}. \end{aligned}$$

We conclude that $h = g^{-Tq}$. Therefore the map τ given by

$$g\tau = \left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-Tq} \end{array}\right),$$

is an isomorphism of $\mathrm{GL}_n(q^2)$ in $\mathrm{GU}_{2n}(q)$.

3. Now let V be a $2n$-dimensional orthogonal vector space over $\mathrm{GF}(q)$ and let Q be the quadratic form on V with Witt index n and let f_Q be its associated bilinear form. Since our quadratic form has Witt index n, there is a basis $v_1, \ldots, v_n, w_1, \ldots, w_n$ of V such that $Q(v_i) = Q(w_i) = 0$ and $f_Q(v_i, w_j) = \delta_{ij}$ by Proposition 2.3.1. We now

argue exactly as in the first case. Let g be a non-singular linear map on $\langle v_1, \ldots, v_n \rangle$ with $v_i g = \sum_{k=1}^{n} g_{ik} v_k$. Again by Witt's Lemma, we can extend g to an isometry of V by setting $w_j h = \sum_{l=1}^{n} h_{jl} w_l$. As before, we require,

$$\begin{aligned}\delta_{ij} &= f_Q(v_i, w_j) = f_Q(v_i g, w_j h) = f_Q\left(\sum_{k=1}^{n} g_{ik} v_k, \sum_{l=1}^{n} h_{jl} w_l\right) \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} g_{ik} h_{jl} f_Q(v_k, w_l) = \sum_{k=1}^{n} g_{ik} h_{jk}.\end{aligned}$$

From this,we can conclude that $h = g^{-T}$. Therefore the map τ given by

$$g\tau = \left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-T} \end{array}\right)$$

is an isomorphism of $\mathrm{GL}_n(q)$ in $\mathrm{GO}_{2n}^{+}(q)$. □

Note that the centre of X is contained in these copies of $\mathrm{GL}_n(q^u)$. Furthermore, these embeddings motivate the following definition.

Definition 3.1.2 Let a be the matrix of a Singer cycle of $\mathrm{GL}_n(q^u)$. Then from the above result, we can find a basis of V such that a embeds in X as

$$\left(\begin{array}{c|c} a & 0 \\ \hline 0 & a^{-T\alpha} \end{array}\right),$$

where

$$\alpha := \begin{cases} q, & \text{if } X = \mathrm{GU}_{2n}(q), \\ 1, & \text{otherwise}. \end{cases}$$

We will refer to the Singer cycle of $\mathrm{GL}_n(q^u)$ inside X as a *linear Singer cycle* of X. We also call the subgroup generated by a linear Singer cycle a *linear Singer subgroup.* We will frequently denote a linear Singer subgroup by $\mathfrak{A}$.

Let V be the underlying vector space of X. Using the above embeddings, we now define group actions of $\mathrm{GL}_n(q^u)$ on V. These can be restricted to the linear Singer subgroups of X. We also show that these actions preserve the forms on V after Proposition 3.2.8.

Suppose first that $X = \mathrm{Sp}_{2n}(q)$ or $\mathrm{GO}^{+}_{2n}(q)$. Then V is a $2n$-dimensional $\mathrm{GF}(q)$-vector space. We let $W = \mathrm{GF}(q^n)$, which we consider as a $\mathrm{GF}(q)$-vector space. We then identify V with $W \oplus W^*$, where W^* denotes the dual space of W. Define an action of $\mathrm{GL}_n(q)$ on V by

$$(v, \theta) \cdot g := \left(vg, g^{-1}\theta\right).$$

This is indeed a group action and if $\tilde{g}$ is the matrix of the action of g on W with respect to some basis of W, then the matrix of the action of g on V is

$$\left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-T} \end{array}\right)$$

so this action agrees with the above embeddings.

Now assume $X = \mathrm{GU}_{2n}(q)$, so V is a $2n$-dimensional $\mathrm{GF}(q^2)$-vector space. This time we let $W = \mathrm{GF}(q^{2n})$, which we consider as a $\mathrm{GF}(q^2)$-vector space and $\sigma : x \to x^q$ be the automorphism of $\mathrm{GF}(q^2)$ of order two. We then identify V with $W \oplus W^{*\sigma}$ where

$$W^{*\sigma} := \{\theta^\sigma := \theta \circ \sigma : \theta \in W^*\}.$$

Define an action of $\mathrm{GL}_n(q^2)$ on V by

$$(v, \theta^\sigma) \cdot g := \left(vg, \left(g^{-1}\theta\right)^\sigma\right).$$

It is easy to check that this is also a group action. Moreover if $\tilde{g}$ is the matrix of the action of g on W with respect to some basis of W, then the matrix of the action of g on

V is

$$\left(\begin{array}{c|c} \tilde{g} & 0 \\ \hline 0 & \tilde{g}^{-T\sigma} \end{array}\right),$$

which also agrees with the above embedding.

It is natural to ask if these actions share any properties with the action of a Singer cycle of $\mathrm{GL}_n(q^u)$ on non-zero vectors of the vector space associated to $\mathrm{GL}_n(q^u)$. We have seen in Chapter 2 that the action of a Singer cycle on the vector space associated to $\mathrm{GL}_n(q^u)$ is transitive on non-zero vectors. However, this is not true for the action of linear Singer cycles of X on the non-zero vectors of V. For example, if

$$\alpha = \begin{cases} \sigma, & \text{if } X = \mathrm{GU}_{2n}(q), \\ 1, & \text{otherwise,} \end{cases}$$

and $\theta \in W^* \setminus \{0\}$, then there is no $a_\lambda \in \mathfrak{A}$ that maps $(1, 0)$ to $(0, \theta^\alpha)$. However, as we will show in the following lemma, this action is still semi-regular and the size of each orbit has length $q^{un} - 1$. We will use this to explicitly describe these orbits.

Lemma 3.1.3 *Suppose that the linear Singer subgroup $\mathfrak{A}$ of X acts on the non-zero vectors of V as above. Let*

$$\alpha = \begin{cases} \sigma, & \textit{if } X = \mathrm{GU}_{2n}(q), \\ 1, & \textit{otherwise.} \end{cases}$$

Then for all $(v, \theta^\alpha) \in V \setminus \{0\}$, we have $\mathrm{Stab}_{\mathfrak{A}}(v, \theta^\alpha) = 1$ and $|\mathrm{Orb}_{\mathfrak{A}}(v, \theta^\alpha)| = q^{un} - 1$.

Proof. Suppose that $a_\lambda \in \mathrm{Stab}_{\mathfrak{A}}(v, \theta^\alpha)$. Then we have

$$(v, \theta^\alpha) = (v, \theta^\alpha) \cdot a_\lambda = (va_\lambda, (a_{\lambda^{-1}}\theta)^\alpha).$$

If $v \neq 0$, then examining the first coordinate, we have

$$va_\lambda - v = v(\lambda - 1) = 0,$$

and so $\lambda = 1$, as required.

Hence, we may assume $v = 0$ and thus $\theta^\alpha \neq 0$. Pick $x \in W \setminus \{0\}$. Then we have

$$\begin{aligned} & (x\theta)^\alpha = ((xa_{\lambda^{-1}})\theta)^\alpha \\ \Rightarrow\ & x\theta = (xa_{\lambda^{-1}})\theta \\ \Rightarrow\ & (x - xa_{\lambda^{-1}})\theta = 0. \end{aligned}$$

This holds for all $\theta \in W^* \setminus \{0\}$, hence

$$x\left(1 - \lambda^{-1}\right) = x - xa_{\lambda^{-1}} = 0.$$

Since $x \neq 0$, we get $\lambda^{-1} = 1$ and so $\mathrm{Stab}_{\mathfrak{A}}(v, \theta^\alpha) = 1$.

Therefore by the Orbit-Stabilizer Theorem, we have

$$|\mathrm{Orb}_{\mathfrak{A}}(v, \theta^\alpha)| = |\mathfrak{A}| / |\mathrm{Stab}_{\mathfrak{A}}(v, \theta^\alpha)| = |\mathfrak{A}| = q^{un} - 1,$$

as required. □

Remark 3.1.4 *Identifying* $W^{*\alpha}$ *with* $\{(0, \theta^\alpha) : \theta^\alpha \in W^{*\alpha}\}$, *a consequence of the above Lemma is that* $\mathrm{Orb}_{\mathfrak{A}}(0, \theta^\alpha) = W^{*\alpha} \setminus \{0\}$. *In particular, if* $(0, \theta^\alpha), (0, \phi^\alpha) \in W^{*\alpha} \setminus \{0\}$, *then there is* $a_\lambda \in \mathfrak{A}$ *such that*

$$(0, \theta^\alpha) = (0, (a_{\lambda^{-1}}\phi)^\alpha) = (0, \phi^\alpha)\, a_\lambda.$$

We are now in a position to describe the orbits of $\mathfrak{A}$.

Proposition 3.1.5 *There are $q^{un}+1$ distinct orbits of $\mathfrak{A}$ on $V\setminus\{0\}$. These are the sets*

$$\mathcal{O}_\infty := \{(0,\theta^\alpha) : \theta^\alpha \in W^{*\alpha}\setminus\{0\}\}$$

and for $\theta \in W^*$,

$$\mathcal{O}_\theta = \{(\lambda, (a_{\lambda^{-1}}\theta)^\alpha) : \lambda \in W\setminus\{0\}\}.$$

Proof. Let m be the number of distinct orbits. Since the orbits partition the set of $q^{2un}-1$ vectors of $V\setminus\{0\}$ and each orbit has length $q^{un}-1$ by Lemma 3.1.3, we have $m(q^{un}-1) = q^{2un}-1$, which gives $m = q^{un}+1$.

Consider the sets $\mathcal{O}_\infty$ and $\mathcal{O}_{\theta.}$. These are indeed orbits as $\mathcal{O}_\theta$ is the orbit of $(1,\theta^\alpha)$ and if $(0,\theta^\alpha),(0,\phi^\alpha) \in \mathcal{O}_\infty$, then there is $a_\lambda \in \mathfrak{A}$ such that

$$(0,\theta^\alpha) = (0,(a_{\lambda^{-1}}\phi)^\alpha) = (0,\phi^\alpha)\cdot a_\lambda.$$

Now if $\mathcal{O}_\theta = \mathcal{O}_\phi$, then $(1,\theta^\alpha) \in \mathcal{O}_\phi$, so there is a $\lambda \in W\setminus\{0\}$ such that $(1,\theta^\alpha) = (\lambda,(a_{\lambda^{-1}}\phi)^\alpha)$. Hence $\lambda = 1$ and so $\theta = \phi$. Therefore the $\mathcal{O}_\theta$ and $\mathcal{O}_\infty$ are all distinct. Since the $\mathcal{O}_\theta$ are indexed by the elements of W^*, these sets are all the $q^{un}+1$ distinct orbits.□

3.2 Invariant subspaces

In Chapter 2, we saw that Singer subgroups of $\mathrm{GL}_n(q)$ act irreducibly on the vector space associated to $\mathrm{GL}_n(q)$. This obviously is not true for linear Singer subgroups of X as

$$W_1 := \{(v,0) : v \in W\}$$

and

$$W_2 := \{(0,\theta^\alpha) : \theta^\alpha \in W^{*\alpha}\}$$

are $\mathfrak{A}$-invariant subspaces of V. It is useful to ask if there are any more invariant subspaces. To this end, we will compute all the $\mathfrak{A}$-invariant subspaces of V. We shall show that except for some small values of n and q, the subspaces, W_1 and W_2 are the only proper non-trivial $\mathfrak{A}$-invariant subspaces of V.

Before we state the main theorem in this section, we need to define some subspaces of V that occur for these small values of n and q.

Definition 3.2.1 *1.* Let $X = \mathrm{Sp}_4(2)$ or $\mathrm{GO}_4^+(2)$, so V is a 4-dimensional $\mathrm{GF}(2)$-vector space. Then

$$W = \mathrm{GF}(4) = \left\{0, 1, \omega, \omega^2\right\},$$

where $\omega^2 + \omega + 1 = 0$ and $W^* = \{0, \theta_1, \theta_\omega, \theta_{\omega^2}\}$, where

$$(1)\,\theta_1 = (\omega)\,\theta_1 = 1, \qquad (1)\,\theta_\omega = 0,\ (\omega)\,\theta_\omega = 1, \qquad (1)\,\theta_{\omega^2} = 1,\ (\omega)\,\theta_{\omega^2} = 0.$$

Then we define the subspaces U_1, U_ω and U_{ω^2} of V as follows:

$$\begin{aligned}
U_1 &:= \left\{(0,0), (1,\theta_1), (\omega,\theta_\omega), \left(\omega^2,\theta_{\omega^2}\right)\right\} = \langle (1,\theta_1), (\omega,\theta_\omega)\rangle, \\
U_\omega &:= \left\{(0,0), (1,\theta_\omega), (\omega,\theta_{\omega^2}), \left(\omega^2,\theta_1\right)\right\} = \langle (1,\theta_\omega), (\omega,\theta_{\omega^2})\rangle, \\
U_{\omega^2} &:= \left\{(0,0), (1,\theta_{\omega^2}), (\omega,\theta_1), \left(\omega^2,\theta_\omega\right)\right\} = \langle (1,\theta_{\omega^2}), (\omega,\theta_1)\rangle.
\end{aligned}$$

2. Let $X = \mathrm{GU}_2(2)$, so V is a 2-dimensional $\mathrm{GF}(4)$-vector space. Then $W = \mathrm{GF}(4)$ as defined above and $W^{*\sigma} = \left\{0, \phi_1^\sigma, \phi_\omega^\sigma, \phi_{\omega^2}^\sigma\right\}$, where

$$(1)\,\phi_1^\sigma = 1, \qquad (1)\,\phi_\omega^\sigma = \omega^2, \qquad (1)\,\phi_{\omega^2}^\sigma = \omega.$$

Then we define the subspaces V_1, V_ω and V_{ω^2} of V as follows:

$$
\begin{aligned}
V_1 &:= \left\{(0,0), (1,\phi_1^\sigma), (\omega,\phi_{\omega^2}^\sigma), \left(\omega^2,\phi_\omega^\sigma\right)\right\} = \langle(1,\phi_1^\sigma)\rangle, \\
V_\omega &:= \left\{(0,0), (1,\phi_\omega^\sigma), (\omega,\phi_1^\sigma), \left(\omega^2,\phi_{\omega^2}^\sigma\right)\right\} = \langle(1,\phi_\omega^\sigma)\rangle, \\
V_{\omega^2} &:= \left\{(0,0), (1,\phi_{\omega^2}^\sigma), (\omega,\phi_\omega^\sigma), \left(\omega^2,\phi_1^\sigma\right)\right\} = \langle(1,\phi_{\omega^2}^\sigma)\rangle.
\end{aligned}
$$

3. Let $X = \mathrm{Sp}_2(3)$ or $\mathrm{GO}_2^+(3)$, so V is a 2-dimensional $\mathrm{GF}(3)$-vector space. Then $W = \mathrm{GF}(3)$ and $W^* = \{0, \iota, -\iota\}$, where $(1)\iota = 1$ and $(1)(-\iota) = -1$. Then we define the subspaces X_1 and X_{-1} by

$$
\begin{aligned}
X_1 &:= \{(0,0), (1,\iota), (-1,-\iota)\} = \langle(1,\iota)\rangle, \\
X_{-1} &:= \{(0,0), (1,-\iota), (-1,\iota)\} = \langle(1,-\iota)\rangle.
\end{aligned}
$$

4. Let $X = \mathrm{Sp}_2(2)$ or $\mathrm{GO}_2^+(2)$, so V is a 2-dimensional $\mathrm{GF}(2)$ vector space. Then $W = \mathrm{GF}(2)$ and $W^* = \{0, \kappa\}$, where $(1)\kappa = 1$. Then we define the subspace Y by

$$Y := \{(0,0), (1,\kappa)\} = \langle(1,\kappa)\rangle$$

We can now classify the $\mathfrak{A}$-invariant subspaces of V.

Theorem 3.2.2 *Suppose that U is an $\mathfrak{A}$-invariant subspace of V. Then either $U \in \{\{0\}, W_1, W_2, V\}$, or one of the following holds:*

1. $X = \mathrm{Sp}_4(2)$ *or* $\mathrm{GO}_4^+(2)$ *and* $U \in \{U_1, U_\omega, U_{\omega^2}\}$;

2. $X = \mathrm{GU}_2(2)$ *and* $U \in \{V_1, V_\omega, V_{\omega^2}\}$;

3. $X = \mathrm{Sp}_2(3)$ *or* $\mathrm{GO}_2^+(3)$ *and* $U \in \{X_1, X_{-1}\}$; *or*

4. $X = \mathrm{Sp}_2(2)$ *or* $\mathrm{GO}_2^+(2)$ *and* $U = Y$.

Before, we prove this theorem, we need the following lemma which says that W_1 and W_2 are irreducible $\mathfrak{A}$-submodules of V.

Lemma 3.2.3 *If U is an $\mathfrak{A}$-invariant subspace of W_1 and $U \neq \{0\}$, then $U = W_1$. Similarly, if U is an $\mathfrak{A}$-invariant subspace of W_2 and $U \neq \{0\}$, then $U = W_2$.*

Proof. Let U be an $\mathfrak{A}$-invariant subspace of W_1 with $U \neq \{0\}$. Then there exists $(v, 0) \in U$ with $v \neq 0$. Then for any $(w, 0) \in W_1$ with $w \neq 0$, we have

$$(w, 0) = (v, 0)\, a_{v^{-1}w} \in U.$$

So $U = W_1$.

Now let U be an $\mathfrak{A}$-invariant subspace of W_2 with $U \neq \{0\}$. Then there exists $(0, \theta^{\alpha}) \in U$ with $\theta^{\alpha} \neq 0$. By Remark 3.1.4, for any $(0, \phi^{\alpha}) \in W_2$ with $\phi^{\alpha} \neq 0$, there is $\lambda \in \mathrm{GF}\left(q^{un}\right)^{\times}$ such that

$$(0, \phi^{\alpha}) = (0, (a_{\lambda^{-1}}\theta)^{\alpha}) = (0, \theta^{\alpha})\, a_{\lambda} \in U.$$

Hence $U = W_2$. $\square$

We now prove Theorem 3.2.2 in a series of propositions.

Proposition 3.2.4 *If U is an $\mathfrak{A}$-invariant subspace of V and $U \cap W_i \neq \{0\}$ for some i, then $U \in \{W_1, W_2, V\}$.*

Proof. Suppose that $U \neq W_1$ or W_2. We will show that $U = V$.

Without loss of generality, assume $U \cap W_1 \neq \{0\}$. Then $U \cap W_1 \leqslant W_1$, so by Lemma 3.2.3, $U \cap W_1 = W_1$ and so $W_1 < U$. Also $V = W_1 \oplus W_2$, so given $x \in U \backslash W_1$, we can write $x = w_1 + w_2$ with $w_i \in W_i$ and $w_2 \neq 0$. Hence

$$w_2 = x - w_1 \in U \cap W_2,$$

so $U \cap W_2 \neq \{0\}$. By Dedekind's Modular Law, we have

$$U = U \cap V = U \cap (W_1 + W_2) = W_1 + (U \cap W_2).$$

But $U \cap W_2 \neq \{0\}$ and $U \cap W_2 \leqslant W_2$, so by Lemma 3.2.3,

$$W_1 + (U \cap W_2) = W_1 + W_2 = V.$$

So $U = V$ as required. □

Proposition 3.2.5 *If U is an $\mathfrak{A}$-invariant subspace of V with $U \cap W_1 = U \cap W_2 = \{0\}$ and $U \neq \{0\}$, then $q \leqslant 3$.*

Proof. Suppose that $(v, \theta^\alpha) \in U$ with v and θ^α non-zero. Then

$$(1, (a_v \theta)^\alpha) = (v, \theta^\alpha)\, a_{v^{-1}} \in U.$$

Since U is a $\mathrm{GF}(q^u)$-subspace of V, for all $\lambda \in \mathrm{GF}(q^u)^\times$, we have

$$\lambda (1, (a_v \theta)^\alpha) = (\lambda, (\lambda^\alpha a_v \theta)^\alpha) \in U$$

and hence, so is $(\lambda, (\lambda^\alpha a_v \theta)^\alpha)\, a_{\lambda^{-1}} = (1, (\lambda \lambda^\alpha a_v \theta)^\alpha)$. This means that

$$(0, ((\lambda \lambda^\alpha - 1)\, a_v \theta)^\alpha) = (1, (\lambda \lambda^\alpha a_v \theta)^\alpha) - (1, (a_v \theta)^\alpha) \in U \cap W_2,$$

so by our assumption $((\lambda \lambda^\alpha - 1)\, a_v \theta)^\alpha = 0$. Since $\theta^\alpha \neq 0$, we can pick $x \in W$ with $(xv)\, \theta \neq 0$. Therefore if $((\lambda \lambda^\alpha - 1)\, a_v \theta)^\alpha = 0$, then $(\lambda \lambda^\alpha - 1)(xv)\, \theta = 0$, so $\lambda \lambda^\alpha - 1 = 0$.

If $X = \mathrm{GU}_{2n}(q)$, then this gives $\lambda^{q+1} = 1$. The number of solutions to this equation in $\mathrm{GF}(q^2)$ is $\gcd(q^2 - 1, q + 1) = q + 1$. On the other hand, by the above argument, every

$\lambda \in \mathrm{GF}(q^2)^\times$ satisfies this equation. Hence $q^2 - 1 = q + 1$ and so $q = 2$.

If $X \neq \mathrm{GU}_{2n}(q)$, then the above equation becomes $\lambda^2 = 1$, so $\lambda = \pm 1$. This forces $q \leqslant 3$. □

Proposition 3.2.6 *If U is a non-zero $\mathfrak{A}$-invariant subspace of V with $U \cap W_1 = U \cap W_2 = \{0\}$ and $q \leqslant 3$, Then one of the following holds:*

1. $X = \mathrm{Sp}_4(2)$ *or* $\mathrm{GO}_4^+(2)$ *and* $U \in \{U_1, U_\omega, U_{\omega^2}\}$;
2. $X = \mathrm{GU}_2(2)$ *and* $U \in \{V_1, V_\omega, V_{\omega^2}\}$;
3. $X = \mathrm{Sp}_2(3)$ *or* $\mathrm{GO}_2^+(3)$ *and* $U \in \{X_1, X_{-1}\}$; *or*
4. $X = \mathrm{Sp}_2(2)$ *or* $\mathrm{GO}_2^+(2)$ *and* $U = Y$.

Proof. If $(v, \theta^\alpha) \in U$ with v and θ^α non-zero, then by the proof of Proposition 3.2.5, $(1, (a_v\theta)^\alpha) \in U$. Hence

$$(1 + v, (a_v\theta + \theta)^\alpha) = (1, (a_v\theta)^\alpha) + (v, \theta^\alpha) \in U.$$

If $v \neq -1$ then

$$(1, (a_{v+1}a_v\theta + a_{v+1}\theta)^\alpha) = (1 + v, (a_v\theta + \theta)^\alpha)\, a_{(v+1)^{-1}} \in U,$$

and so

$$(0, (a_{v+1}a_v\theta + a_{v+1}\theta - a_v\theta)^\alpha) = (1, (a_{v+1}a_v\theta + a_{v+1}\theta)^\alpha) - (1, (a_v\theta)^\alpha) \in U \cap W_2.$$

By our assumptions we must have $a_{v+1}a_v\theta + a_{v+1}\theta - a_v\theta = 0$. This means, for all $x \in W$, we have

$$\begin{aligned}0 &= (x)\left(a_{v+1}a_v\theta + a_{v+1}\theta - a_v\theta\right) \\ &= (x)\left(a_{v+1}a_v\theta\right) + (x)\left(a_{v+1}\theta\right) - (x)\left(a_v\theta\right) \\ &= \left(x\left(v+1\right)v\right)\theta + \left(x\left(v+1\right)\right)\theta - \left(xv\right)\theta \\ &= \left(x\left(v^2+v+1\right)\right)\theta.\end{aligned}$$

Since $\theta \neq 0$, this yields $v^2+v+1=0$. Therefore either $v=-1$ or v^3-1.

If $X = \mathrm{GU}_{2n}(q)$, then by the proof of Proposition 3.2.5, $v \in \mathrm{GF}\left(2^{2n}\right)^{\times}$ and the number of solutions to $v^3=1$ in $\mathrm{GF}\left(2^{2n}\right)$ is $\gcd\left(2^{2n}-1,3\right)=3$. On the other hand, by the above argument, every element of $\mathrm{GF}\left(2^{2n}\right)^{\times}$ satisfies $v^3=1$. This forces $2^{2n}-1=3$ and so $n=1$ and $X=\mathrm{GU}_2(2)$. This means $W=\mathrm{GF}(4)$ and $W^{*\sigma}=\left\{0,\phi_1^{\sigma},\phi_{\omega}^{\sigma},\phi_{\omega^2}^{\sigma}\right\}$, as defined in Definition 3.2.1.

Without loss of generality, assume that $v=1$. If $\theta^{\sigma}=\phi_1^{\sigma}$, then since U is $\mathfrak{A}$-invariant,

$$U=\left\{(0,0),\left(1,\phi_1^{\sigma}\right),\left(\omega,\phi_{\omega^2}^{\sigma}\right),\left(\omega^2,\phi_{\omega}^{\sigma}\right)\right\}=V_1,$$

if $\theta^{\sigma}=\phi_{\omega}^{\sigma}$, then

$$U=\left\{(0,0),\left(1,\phi_{\omega}^{\sigma}\right),\left(\omega,\phi_1^{\sigma}\right),\left(\omega^2,\phi_{\omega^2}^{\sigma}\right)\right\}=V_{\omega},$$

and if $\theta^{\sigma}=\phi_{\omega^2}^{\sigma}$, then

$$U=\left\{(0,0),\left(1,\phi_{\omega^2}^{\sigma}\right),\left(\omega,\phi_{\omega}^{\sigma}\right),\left(\omega^2,\phi_1^{\sigma}\right)\right\}=V_{\omega^2},$$

as required.

Hence $X \neq \mathrm{GU}_{2n}(q)$. If $q=3$, then the only element in $\mathrm{GF}\left(3^n\right)^{\times}$ which satisfies $v^3=1$ is $v=1$. Therefore $v\in\{-1,1\}$ and so $n=1$ and $X=\mathrm{Sp}_2(3)$ or $\mathrm{GO}_2^{+}(3)$. This means $W = \mathrm{GF}(3)$ and $W^* = \{0, \iota, -\iota\}$, as defined in Definition 3.2.1.

As above, we can assume $v = 1$. If $\theta = \iota$, then as U is $\mathfrak{A}$-invariant,

$$U = \{(0,0), (1,\iota), (-1,-\iota)\} = X_1,$$

and if $\theta = -\iota$, then

$$U = \{(0,0), (1,-\iota), (-1,\iota)\} = X_{-1},$$

as required.

Therefore $q = 2$. If n is odd, then the only element in $\mathrm{GF}(2^n)$, which satisfies $v^3 = 1$ is $v = 1$. Therefore $n = 1$ and $X = \mathrm{Sp}_2(2)$ or $\mathrm{GO}_2^+(2)$. This means $W = \mathrm{GF}(2)$ and $W^* = \{0, \kappa\}$, as defined in Definition 3.2.1. Hence $(v, \theta) = (1, \kappa)$ and so

$$U = \{(0,0), (1,\kappa)\} = Y,$$

as required.

All thats left to consider is the case when n is even. Here the number of solutions to $v^3 = 1$ in $\mathrm{GF}(2^n)$ is $\gcd(2^n - 1, 3) = 3$. By the above argument, every element of $\mathrm{GF}(2^n)^\times$ satisfies $v^3 = 1$. We therefore have $2^n - 1 = 3$, so $n = 2$ and $X = \mathrm{Sp}_4(2)$ or $\mathrm{GO}_4^+(2)$. Hence $W = \mathrm{GF}(4)$ and $W^* = \{0, \theta_1, \theta_\omega, \theta_{\omega^2}\}$, as defined in Definition 3.2.1.

Again we can assume that $v = 1$. If $\theta = \theta_1$, then since U is $\mathfrak{A}$-invariant,

$$U = \left\{(0,0), (1,\theta_1), (\omega,\theta_\omega), \left(\omega^2,\theta_{\omega^2}\right)\right\} = U_1,$$

if $\theta = \theta_\omega$, then

$$U = \left\{(0,0), (1,\theta_\omega), (\omega,\theta_{\omega^2}), \left(\omega^2,\theta_1\right)\right\} = U_\omega,$$

and if $\theta = \theta_{\omega^2}$, then

$$U = \left\{ (0,0), (1, \theta_{\omega^2}), (\omega, \theta_1), \left(\omega^2, \theta_\omega\right) \right\} = U_{\omega^2}.$$

This concludes the proof of the proposition and the proof of Theorem 3.2.2. □

As a result of Theorem 3.2.2, we can make the following observation.

Corollary 3.2.7 *If U is a proper non-trivial $\mathfrak{A}$-subspace of V, then $\mathfrak{A}$ is transitive on non-zero vectors of U.*

Proof. If $U = W_1$, then for any $(v,0), (w,0) \in W_1$ with $v, w \neq 0$, we have $(w,0) = (v,0)\, a_{v^{-1}w}$. Hence $\mathfrak{A}$ is transitive on non-zero vectors of W_1. If $U = W_2$, then $\mathfrak{A}$ is transitive on nonzero vectors of U by Remark 3.1.4. Finally, if

$$U \in \{U_1, U_\omega, U_{\omega^2}, V_1, V_\omega, V_{\omega^2}, X_1, X_{-1}, Y\},$$

then it is obvious from Definition 3.2.1 that $\mathfrak{A}$ is transitive on non-zero vectors of U. □

It is useful to know which of the proper non-trivial $\mathfrak{A}$-invariant subspaces are non-degenerate, and which are totally singular. To determine this, we need to define symplectic, unitary and quadratic forms on V. The following proposition gives the forms we require.

Proposition 3.2.8 *Let V be the vector space associated to X.*

1. *If $X = \mathrm{Sp}_{2n}(q)$, then the function $f_S : V \times V \to \mathrm{GF}(q)$ defined by*

$$f_S((v,\theta), (w,\phi)) = v\phi - w\theta,$$

is a symplectic form on V

2. *If* $X = \mathrm{GU}_{2n}(q)$*, then the function* $f_U : V \times V \to \mathrm{GF}(q^2)$ *defined by*

$$f_U((v, \theta^\sigma), (w, \phi^\sigma)) = v\phi + w\theta^\sigma,$$

is a unitary form on V

3. *If* $X = \mathrm{GO}^+_{2n}(q)$*, then the function* $Q : V \to \mathrm{GF}(q)$ *defined by*

$$Q((v, \theta)) = v\theta,$$

is a non-degenerate quadratic form on V *of plus type.*

Proof. 1. We have

$$f_S((v, \theta), (v, \theta)) = v\theta - v\theta = 0,$$

and

$$f_S((w, \phi), (v, \theta)) = w\theta - v\phi = -(v\phi - w\theta) = -f_S((v, \theta), (w, \phi)),$$

for all $(v, \theta), (w, \phi) \in V$. Also, for all $(v, \theta), (w, \phi), (x, \psi) \in V$ and $\lambda \in \mathrm{GF}(q)$, we have

$$\begin{aligned} f_S((v, \theta) + \lambda(w, \phi), (x, \psi)) &= (v + \lambda w)\psi - x(\theta + \lambda\phi) \\ &= v\psi - x\theta + \lambda(w\psi - x\phi) \\ &= f_S((v, \theta), (x, \psi)) + \lambda f_S((w, \phi), (x, \psi)). \end{aligned}$$

Therefore f_S is a skew-symmetric, alternating bilinear form.

Now, let $(v, \theta) \in \mathrm{Rad}(f_S)$. So for all $(w, \phi) \in V$, we have

$$f_S((v, \theta), (w, \phi)) = v\phi - w\theta = 0.$$

In particular setting $w = 0$, we get $v\phi = 0$ for all $\phi \in W^*$, which implies $v = 0$. Hence $w\theta = 0$ for all $w \in W$, and so $\theta = 0$. Therefore $\mathrm{Rad}\,(f_S) = 0$ and f_S is non-degenerate, so f_S is a symplectic form on V.

2. This time, we have

$$f_U\left((w, \phi^\sigma), (v, \theta^\sigma)\right) = w\theta + v\phi^\sigma = (w\theta^\sigma + v\phi)^\sigma = \left(f_U\left((v, \theta^\sigma), (w, \phi^\sigma)\right)\right)^\sigma,$$

for all $(v, \theta^\sigma), (w, \phi^\sigma) \in V$.

Also, for all $(v, \theta^\sigma), (w, \phi^\sigma), (x, \psi^\sigma) \in V$ and $\lambda \in \mathrm{GF}\,(q^2)$, we have

$$\begin{aligned} f_U\left((v, \theta^\sigma) + \lambda (w, \phi^\sigma), (x, \psi^\sigma)\right) &= (v + w)\,\psi + x\,(\theta^\sigma + \lambda\phi^\sigma) \\ &= v\psi + x\theta^\sigma + \lambda\,(w\psi + x\phi^\sigma) \\ &= f_U\left((v, \theta^\sigma), (x, \psi^\sigma)\right) + \lambda f_U\left((w, \phi^\sigma), (x, \psi^\sigma)\right), \end{aligned}$$

so f_U is a conjugate-symmetric sesquilinear form. A similar sort of argument as before shows that f_U is non-degenerate so f_U is in fact a unitary form.

3. Define $f_Q : V \times V \to \mathrm{GF}\,(q)$ by

$$\begin{aligned} f_Q\left((v, \theta), (w, \phi)\right) &:= Q\left((v, \theta) + (w, \phi)\right) - Q\left((v, \theta)\right) - Q\left((w, \phi)\right) \\ &= (v + w)\,(\theta + \phi) - v\theta - w\phi \\ &= v\phi + w\theta \end{aligned}$$

Then for all $(v, \theta), (w, \phi), (x, \psi) \in V$ and $\lambda \in \mathrm{GF}\,(q)$, we have

$$f_Q\left((w, \phi), (v, \theta)\right) = f_Q\left((v, \theta), (w, \phi)\right)$$

and

$$
\begin{aligned}
f_Q\left((v,\theta)+\lambda(w,\phi),(x,\psi)\right) &= (v+\lambda w)\psi + x(\theta+\lambda\phi) \\
&= v\psi + x\theta + \lambda(w\psi + x\phi) \\
&= f_Q\left((v,\theta),(x,\psi)\right) + \lambda f_Q\left((w,\phi),(x,\psi)\right),
\end{aligned}
$$

Therefore f_Q is a symmetric bilinear form

Also, if $(v,\theta)\in V$ and $\lambda\in \mathrm{GF}(q)$ then,

$$
Q\left(\lambda(v,\theta)\right) = (\lambda v)(\lambda\theta) = \lambda^2(v\theta) = \lambda^2 Q\left((v,\theta)\right).
$$

Therefore Q is a quadratic form on V. By the same argument as in the symplectic case, f_Q is non-degenerate and so Q is non-degenerate.

Finally, if W_1 is the subspace of V defined in Theorem 3.2.2, then $\dim(W_1) = n$ and for all $(v,0)\in W_1$, we have $Q((v,0)) = 0$, so Q has plus type. □

As an aside, if $g\in \mathrm{GL}_n(q^u)$, then if $X = \mathrm{Sp}_{2n}(q)$, we have

$$
\begin{aligned}
f_S\left((v,\theta)g,(w,\phi)g\right) &= f_S\left(\left(vg, g^{-1}\theta\right),\left(wg, g^{-1}\phi\right)\right) \\
&= \left(vgg^{-1}\right)\phi - \left(wgg^{-1}\right)\theta \\
&= v\phi - w\theta \\
&= f_S\left((v,\theta),(w,\phi)\right).
\end{aligned}
$$

If $X = \mathrm{GO}^+_{2n}(q)$, then

$$
Q\left((v,\theta)g\right) = vgg^{-1}\theta = v\theta = Q\left((v,\theta)\right),
$$

and if $X = \mathrm{GU}_{2n}(q)$, then

$$\begin{aligned} f_U\left(\left(v,\theta^\sigma\right)g,\left(w,\phi^\sigma\right)g\right) &= f_U\left(\left(vg,\left(g^{-1}\theta\right)^\sigma\right),\left(wg,\left(g^{-1}\phi\right)^\sigma\right)\right) \\ &= vgg^{-1}\phi + wg\left(g^{-1}\theta\right)^\sigma \\ &= v\phi + w\theta^\sigma \\ &= f_U\left(\left(v,\theta^\sigma\right),\left(w,\phi^\sigma\right)\right). \end{aligned}$$

so our actions of $\mathrm{GL}_n(q^u)$ preserve the forms on V. In particular, so does $\mathfrak{A}$.

Proposition 3.2.9 *1. If $X = \mathrm{Sp}_{2n}(q)$, then the subspaces W_1, W_2, U_ω, X_1, X_{-1} and Y are isotropic. The subspaces U_1 and U_{ω^2} are non-degenerate.*

2. If $X = \mathrm{GU}_{2n}(q)$, then the subspaces W_1, W_2 and V_1 are isotropic. The subspaces V_ω and V_{ω^2} are non-degenerate.

3. If $X = \mathrm{GO}^+_{2n}(q)$, then the subspaces W_1, W_2 and U_ω are singular. The subspaces U_1, U_{ω^2}, X_1, X_{-1} and Y are non-singular.

Proof. 1. Note that for all $(v,0),(w,0) \in W_1$, we have

$$f_S\left((v,0),(w,0)\right) = (v)\,0 - (w)\,0 = 0,$$

and for all $(0,\theta),(0,\phi) \in W_2$, we get

$$f_S\left((0,\theta),(0,\phi)\right) = (0)\,\phi - (0)\,\theta = 0.$$

Therefore the subspaces W_1 and W_2 are isotropic. Also since f_S is bilinear and alternating, any 1-space in V is isotropic. This means X_1, X_{-1} and Y are isotropic.

Now $(1, \theta_1), (\omega, \theta_\omega) \in U_1$ and

$$f_S((1, \theta_1), (\omega, \theta_\omega)) = (1)\,\theta_\omega - (\omega)\,\theta_1 = 1.$$

Similarly $(1, \theta_{\omega^2}), (\omega, \theta_1) \in U_{\omega^2}$ and

$$f_S((1, \theta_{\omega^2}), (\omega, \theta_1)) = (1)\,\theta_1 - (\omega)\,\theta_{\omega^2} = 1.$$

Therefore the subspaces U_1 and U_{ω^2} are non-degenerate. This leaves the subspace U_ω. Since f_S is a symplectic form, we only need to compute $f_S((1, \theta_\omega), (\omega, \theta_{\omega^2}))$. We have

$$f_S((1, \theta_\omega), (\omega, \theta_{\omega^2})) = (1)\,\theta_{\omega^2} - (\omega)\,\theta_\omega = 1 - 1 = 0.$$

Therefore U_ω is isotropic.

2. For all $(v, 0), (w, 0) \in W_1$, we have

$$f_U((v, 0), (w, 0)) = (v)\,0 - (w)\,0 = 0,$$

and for all $(0, \theta^\sigma), (0, \phi^\sigma) \in W_2$, we get

$$f_U((0, \theta^\sigma), (0, \phi^\sigma)) = (0)\,\phi - (0)\,\theta^\sigma = 0.$$

Hence the subspaces W_1 and W_2 are isotropic. Now $(1, \phi_\omega^\sigma) \in V_\omega$ and $\left(1, \phi_{\omega^2}^\sigma\right) \in V_{\omega^2}$, so

$$f_U((1, \phi_\omega^\sigma), (1, \phi_\omega^\sigma)) = (1)\,\phi_\omega + (1)\,\phi_\omega^\sigma = \omega + \omega^2 = 1$$

and

$$f_U((1, \phi_{\omega^2}^\sigma), (1, \phi_{\omega^2}^\sigma)) = (1)\,\phi_{\omega^2} + (1)\,\phi_{\omega^2}^\sigma = \omega^2 + \omega = 1.$$

Hence the subspaces V_ω and V_{ω^2} are non-degenerate. This leaves V_1. Since f_U is a unitary form, we only need to compute $f_U\left(\left(1, \phi_1^\sigma\right), \left(1, \phi_1^\sigma\right)\right)$. We have

$$f_U\left(\left(1, \phi_1^\sigma\right), \left(1, \phi_1^\sigma\right)\right) = (1)\,\phi_1 + (1)\,\phi_1^\sigma = 1 + 1 = 0,$$

as $f_U\left(\left(1, \phi_1^\sigma\right), \left(1, \phi_1^\sigma\right)\right)$ lies in $\mathrm{GF}(4)$. Therefore V_1 is isotropic.

3. For all $(v, 0) \in W_1$ and $(0, \theta) \in W_2$, we have

$$Q\,(v, 0) = (v)\,0 = 0$$

and

$$Q\,(0, \theta) = (0)\,\theta = 0.$$

Hence the subspaces W_1 and W_2 are singular. Also $(1, \theta_1) \in U_1$ and $(1, \theta_{\omega^2}) \in U_{\omega^2}$ so

$$Q\,(1, \theta_1) = (1)\,\theta_1 = 1$$

and

$$Q\,(1, \theta_{\omega^2}) = (1)\,\theta_{\omega^2} = 1.$$

Hence U_1 and U_{ω^2} are non-singular. Similarly

$$Q\,(1, \iota) = (1)\,\iota = 1,$$

$$Q\,(1, -\iota) = (1)\,(-\iota) = -1,$$

and

$$Q\,(1, \kappa) = (1)\,\kappa = 1,$$

so X_1, X_{-1} and Y are also non-singular. This leaves the subspace U_ω. We have

$$Q\left(1,\theta_\omega\right) = (1)\,\theta_\omega = 0,$$

$$Q\left(\omega,\theta_{\omega^2}\right) = (\omega)\,\theta_{\omega^2} = 0$$

and

$$Q\left(\omega^2,\theta_1\right) = \left(\omega^2\right)\theta_1 = 0.$$

Therefore U_ω is singular. □

As a remark, if $U = U_1$, V_ω or X_1, then it it easy to see that $U^\perp = U_{\omega^2}$, V_{ω^2} or X_{-1}, respectively.

3.3 Centralizers and normalizers

We conclude this chapter by using our classification of the invariant subspaces to compute the centralizer and normalizer of the linear Singer cycle of X.

From [24, the proofs of Lemma 4.1.9 and Corollary 4.2.2], the stabilizer of the direct sum $W_1 \oplus W_2$ in X is

$$\mathrm{GL}_n\left(q^u\right).2 = \left\langle \left(\begin{array}{c|c} g & 0 \\ \hline 0 & g^{-T\alpha} \end{array}\right), \left(\begin{array}{c|c} 0 & I \\ \hline \pm I & 0 \end{array}\right) : g \in \mathrm{GL}_n\left(q^u\right) \right\rangle,$$

where the sign is negative, when $X = \mathrm{Sp}_{2n}(q)$ and positive, when $X \neq \mathrm{Sp}_{2n}(q)$. For $n \geqslant 2$, we define the group $\Gamma\mathrm{L}_1\left(q^{un}/q^u\right).2$ as the subgroup of $\mathrm{GL}_n\left(q^u\right).2$ given by

$$\Gamma\mathrm{L}_1\left(q^{un}/q^u\right).2 = \left\langle \left(\begin{array}{c|c} \gamma & 0 \\ \hline 0 & \gamma^{-T\alpha} \end{array}\right), \left(\begin{array}{c|c} 0 & I \\ \hline \pm I & 0 \end{array}\right) : \gamma \in \Gamma\mathrm{L}_1\left(q^{un}/q^u\right) \right\rangle,$$

where $\Gamma\mathrm{L}_1\left(q^{un}/q^u\right)$ is defined in Chapter 2.

Proposition 3.3.1 *Suppose that X is not one of* $\mathrm{GU}_2(2)$, $\mathrm{Sp}_4(2)$, $\mathrm{GO}_4^+(2)$, $\mathrm{Sp}_2(3)$, $\mathrm{GO}_2^+(3)$, $\mathrm{Sp}_2(2)$ *or* $\mathrm{GO}_2^+(2)$. *If $\mathfrak{A}$ is the linear Singer subgroup of X, then*

$$\mathrm{N}_X(\mathfrak{A}) = \begin{cases} \mathrm{GL}_1(q^{un}).2, & \textit{if } n=1, \\ \Gamma\mathrm{L}_1(q^{un}/q^u).2, & \textit{otherwise.} \end{cases}$$

Proof. Let $N = \mathrm{N}_X(\mathfrak{A})$ and suppose $n \in N$. If W_1 is the subspace defined in Theorem 3.2.2, then the image under n, $W_1 n$ is also a subspace of V. Let $a \in \mathfrak{A}$ and $(v,0) \in W_1$. Then since $a^{n^{-1}} \in \mathfrak{A}$ and W_1 is $\mathfrak{A}$-invariant, we have

$$(v,0)\, na = (v,0)\, a^{n^{-1}} n \in W_1 n.$$

Therefore $W_1 n$ is an $\mathfrak{A}$-invariant subspace of V, so since by our assumptions, we have $W_1 n \in \{W_1, W_2\}$ by Theorem 3.2.2. Similarly, $W_2 n$ is also $\mathfrak{A}$-invariant, and so $W_2 n \in \{W_1, W_2\}$.

Now, n either fixes the W_i or swaps them, for if $W_1 n = W_1$ and $W_2 n = W_1$, then since n has finite order e, we have

$$W_2 = W_2 n^e = W_1 n^{e-1} = \ldots = W_1 n = W_1,$$

which is a contradiction. Similarly, we cannot have $W_1 n = W_2$ and $W_2 n = W_2$. This means that N preserves the direct sum $W_1 \oplus W_2$ and so lies its stabilizer, $\mathrm{GL}_n(q^u).2$.

For $a \in \mathfrak{A}$, we have

$$\left(\begin{array}{c|c} 0 & I \\ \hline -I & 0 \end{array}\right)^{-1} \left(\begin{array}{c|c} a & 0 \\ \hline 0 & a^{-T\alpha} \end{array}\right) \left(\begin{array}{c|c} 0 & I \\ \hline -I & 0 \end{array}\right) = \left(\begin{array}{c|c} a^{-T\alpha} & 0 \\ \hline 0 & a \end{array}\right) \in \mathfrak{A}.$$

Also by Proposition 2.1.6, if $g \in \mathrm{GL}_n(q^u)$ normalizes $\mathfrak{A}$, then

$$g \in \begin{cases} \mathrm{GL}_1(q^u), & \text{if } n = 1, \\ \Gamma\mathrm{L}_1(q^{un}/q^u), & \text{otherwise.} \end{cases}$$

Therefore

$$\mathrm{N}_X(\mathfrak{A}) = \begin{cases} \mathrm{GL}_1(q^u).2, & \text{if } n = 1, \\ \Gamma\mathrm{L}_1(q^{un}/q^u).2, & \text{otherwise,} \end{cases}$$

as required. □

Corollary 3.3.2 *Suppose X is not one of* $\mathrm{GU}_2(2)$, $\mathrm{Sp}_4(2)$, $\mathrm{GO}_4^+(2)$, $\mathrm{Sp}_2(3)$, $\mathrm{GO}_2^+(3)$, $\mathrm{Sp}_2(2)$ *or* $\mathrm{GO}_2^+(2)$. *If $\mathfrak{A}$ is the linear Singer subgroup of X, then* $\mathrm{C}_X(\mathfrak{A}) = \mathfrak{A}$.

Proof. Since $\mathrm{C}_X(\mathfrak{A}) \leqslant \mathrm{N}_X(\mathfrak{A})$, we have $\mathrm{C}_X(\mathfrak{A}) \leqslant \mathrm{GL}_n(q^u).2$, by Proposition 3.3.1.

By the proof of Proposition 3.3.1, the element

$$\left(\begin{array}{c|c} 0 & I \\ \hline -I & 0 \end{array}\right)$$

does not centralize $\mathfrak{A}$. On the other hand, if $g \in \mathrm{GL}_n(q^u)$ centralizes $\mathfrak{A}$, then $g \in \mathfrak{A}$, by Lemma 2.1.5. Therefore $\mathrm{C}_X(\mathfrak{A}) = \mathfrak{A}$. □

Note that if $X = \mathrm{GO}_2^+(q)$, then by considering orders, we have $\mathrm{N}_X(\mathfrak{A}) = X$.

The exceptional cases are easy to deal with. If $X = \mathrm{GU}_2(2)$, $\mathrm{Sp}_2(3)$ or $\mathrm{Sp}_2(2)$, then $\mathfrak{A} = \mathrm{Z}(X)$ and so $\mathrm{N}_X(\mathfrak{A}) = \mathrm{C}_X(\mathfrak{A}) = X$. Similarly, if $X = \mathrm{GO}_2^+(3)$ or $\mathrm{GO}_2^+(2)$, then as X is abelian, we also have $\mathrm{N}_X(\mathfrak{A}) = \mathrm{C}_X(\mathfrak{A}) = X$. Finally, if $X = \mathrm{Sp}_4(2)$ or $\mathrm{GO}_4^+(2)$, then the linear Singer cycle of X has order 3. Hence $C_X(\mathfrak{A}) = \mathrm{S}_3 \times 3$ and

$$N_X(\mathfrak{A}) = \mathrm{S}_3 \times \mathrm{S}_3 \cong \Omega_4^+(2).$$

Chapter 4

Statement of the main theorems and small dimensional cases

In this chapter we give the main theorems of this thesis. We also deal with the cases in small dimensions.

4.1 Main theorems

We now state the main theorems which are the subject of this thesis.

Theorem 4.1.1 *Let $n \geqslant 2$ and let $G \leqslant \mathrm{Sp}_{2n}(q)$. Suppose that G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. Then one of the following holds:*

1. *$G \in \mathcal{C}_1$ and G is contained in either $\mathrm{Stab}_{\mathrm{Sp}_{2n}(q)}(W_1)$ or $\mathrm{Stab}_{\mathrm{Sp}_{2n}(q)}(W_2)$ or when $(n, q) = (2, 2)$, G is contained in $\mathrm{Stab}_{\mathrm{Sp}_4(2)}(U_\omega)$. All groups have the structure $q^{n(n+1)/2} : \mathrm{GL}_n(q)$ in $\mathrm{Sp}_{2n}(q)$;*

2. *$G \in \mathcal{C}_2$ and G is contained in $\mathrm{GL}_n(q).2$, with q odd;*

3. *$G \in \mathcal{C}_3$ and G is contained in $\mathrm{Sp}_{2n/s}(q^s).s$, where s is a prime dividing n;*

4. *$G \in \mathcal{C}_3$ and G is contained in $\mathrm{GU}_n(q).2$, with n even and q odd;*

5. $G \in \mathcal{C}_8$ *and* G *is contained in* $\mathrm{GO}_{2n}^{+}(q)$, *with* q *even;*

6. $G \in \mathcal{C}_1$, $(n, q) = (2, 2)$ *and* G *is contained in* $\mathrm{Stab}_{\mathrm{Sp}_4(2)}(U_1) = \mathrm{Stab}_{\mathrm{Sp}_4(2)}(U_{\omega^2})$. *This group is isomorphic to* $\mathrm{Sp}_2(2) \times \mathrm{Sp}_2(2) \cong \mathrm{S}_3 \times \mathrm{S}_3$;

7. $G \in \mathcal{C}_2$, $(n, q) = (2, 2)$ *or* $(2, 3)$ *and* G *is contained in* $\mathrm{Sp}_2(q) \wr \mathrm{S}_2$;

8. $G \in \mathcal{C}_6$, $(n, q) = (2, 3)$ *and* G *is contained in* $2_{-}^{1+4}.\Omega_4^{-}(2) \cong 2_{-}^{1+4}.\mathrm{A}_5$;

9. $G \in \mathcal{S}$, $(n, q) = (2, 2)$ *and* $G = \mathrm{A}_6 = \mathrm{Sp}_{2n}(q)'$;

10. $G \in \mathcal{S}$, $(n, q) = (3, 2)$ *and* $\mathrm{PSU}_3(3) \leqslant G \leqslant \mathrm{PSU}_3(3) : 2$; *or*

11. $G \in \mathcal{S}$, $(n, q) = (3, 3)$ *and* G *is is one of two copies of* $\mathrm{SL}_2(13)$.

Theorem 4.1.2 *Let* $n \geqslant 2$ *and let* $G \leqslant \mathrm{GU}_{2n}(q)$. *Suppose that* G *contains a linear Singer cycle of* $\mathrm{GU}_{2n}(q)$. *Then one of the following holds:*

1. $G \in \mathcal{C}_1$ *and* G *is contained in either* $\mathrm{Stab}_{\mathrm{GU}_{2n}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{GU}_{2n}(q)}(W_2)$. *Both groups have the structure* $q^{n^2} : \mathrm{GL}_n(q^2)$;

2. $G \in \mathcal{C}_2$ *and* G *is contained in* $\mathrm{GL}_n(q^2).2$;

3. $G \in \mathcal{C}_3$ *and* G *is contained in* $\mathrm{GU}_{2n/s}(q^s).s$, *where* s *is an odd prime; or*

4. $G \in \mathcal{C}_5$, $(n, q) = (2, 2)$ *and* G *is contained in* $C_3 \circ \mathrm{Sp}_4(2) \cong 3 \times \mathrm{S}_6$.

Theorem 4.1.3 *Let* $n \geqslant 3$ *and let* G *be a subgroup of* $\mathrm{GO}_{2n}^{+}(q)$ *not containing* $\Omega_{2n}^{+}(q)$. *Suppose that* G *contains a linear Singer cycle of* $\mathrm{GO}_{2n}^{+}(q)$.*Then one of the following holds:*

1. $G \in \mathcal{C}_1$ *and* G *is contained in either* $\mathrm{Stab}_{\mathrm{GO}_{2n}^{+}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{GO}_{2n}^{+}(q)}(W_2)$. *Both groups have the structure* $q^{n(n-1)/2} : \mathrm{GL}_n(q)$;

2. $G \in \mathcal{C}_2$ *and* G *is contained in* $\mathrm{GL}_n(q).2$;

3. $G \in \mathcal{C}_3$ *and* G *is contained in* $\mathrm{GO}^{+}_{2n/s}(q^s).s$*, where* s *is a prime dividing* n*;*

4. $G \in \mathcal{C}_3$ *and* G *is contained in* $\mathrm{GU}_n(q).2$*, with* n *even;*

5. $G \in \mathcal{C}_4$*,* $(n,q) = (4,2)$ *and* G *is contained in* $\mathrm{Sp}_4(2) \circ \mathrm{Sp}_2(2) \cong \mathrm{S}_6 \times \mathrm{S}_3$*;*

6. $G \in \mathcal{S}$*,* $(n,q) = (3,2)$ *and* $\mathrm{A}_7 \leqslant G \leqslant \mathrm{S}_7$*; or*

7. $G \in \mathcal{S}$*,* $(n,q) = (4,2)$ *and* $G = \mathrm{A}_9$*.*

From these, we can deduce that if n is large and G is as stated in the main theorems, then G is contained in

$$\begin{cases} \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_8, & \text{if } X = \mathrm{Sp}_{2n}(q), \\ \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3, & \text{otherwise.} \end{cases}$$

The group $\mathrm{GL}_n(q^u).2$ is just the stabilizer of the direct sum $W_1 \oplus W_2$. The groups $\mathrm{Sp}_{2n/s}(q^s).s$, $\mathrm{GU}_{2n/s}(q^s).s$ and $\mathrm{GO}^{+}_{2n/s}(q^s).s$ are analogous to the groups in Theorem 2.1.4. These arise in a similar way: we take a $2n/s$-dimensional $\mathrm{GF}(q^{us})$-vector space, V' and consider it as a $2n$-dimensional $\mathrm{GF}(q^u)$-vector space, V. We then take a symplectic, unitary or orthogonal form, κ' on V' and construct a symplectic, unitary or quadratic form, κ on V, respectively, by putting $\kappa = \kappa' \mathrm{Tr}^{\mathrm{GF}(q^{us})}_{\mathrm{GF}(q^u)}$, where $\mathrm{Tr}^{\mathrm{GF}(q^{us})}_{\mathrm{GF}(q^u)}$ is the trace map from $\mathrm{GF}(q^{us})$ to $\mathrm{GF}(q^u)$. Then any isometry of V' can be viewed as an isometry of V.

The $\mathrm{GU}_n(q).2$ subgroups arise in a similar way. We take a unitary form on a unitary space and use it to construct a symplectic or quadratic form and then view the isometries of $\mathrm{GU}_n(q)$ as elements of $\mathrm{Sp}_{2n}(q)$ and $\mathrm{GO}^{+}_{2n}(q)$.

The subgroup, $\mathrm{GO}^{+}_{2n}(q)$ of $\mathrm{Sp}_{2n}(q)$ arises since the associated bilinear form of a quadratic form is skew-symmetric and alternating in characteristic 2.

The proof of Theorems 4.1.1, 4.1.2 and 4.1.3 constitutes Chapters 5 and 6. In Chapter 5, we distinguish between the cases when $X = \mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}^{+}_{2n}(q)$ for clarity. In Chapter 6 however, we consider these together until we need to consider specific cases.

4.2 The case when $n = 1$

For the remainder of this chapter, we concern ourselves with the small dimensional cases. In this section, we assume that $n = 1$. We do not need to consider $X = \mathrm{GO}_2^+(q)$, as then $X \cong \mathrm{D}_{2(q-1)}$ and the result is obvious, so we assume that $X = \mathrm{Sp}_2(q)$ or $\mathrm{GU}_2(q)$. Since $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$ and $\mathrm{PSU}_2(q) \cong \mathrm{PGL}_2(q)$, these cases are just an application of Theorems 2.4.1 and 2.4.2. In contrast to Theorems 4.1.1, 4.1.2 and 4.1.3, we can compute all the overgroups of the linear Singer cycle in these cases.

Theorem 4.2.1 *Suppose that G is a proper subgroup of $\mathrm{Sp}_2(q)$ containing a linear Singer cycle of $\mathrm{Sp}_2(q)$. Then up to conjugacy, one of the following holds:*

1. $G = \mathrm{GL}_1(q)$, *the linear Singer subgroup;*

2. $G \in \mathcal{C}_1$ *and* $G = q : \mathrm{GL}_1(q)$*;*

3. $G \in \mathcal{C}_2$ *and* $G = \mathrm{GL}_1(q).2$, *for q odd;*

4. $G \in \mathcal{C}_8$ *and* $G = \mathrm{GO}_2^+(q)$, *for q even;*

5. $G \in \mathcal{C}_3$, $q = 2$ *and* $G = \mathrm{GU}_1(2)$*;*

6. $G \in \mathcal{C}_3$, $q = 3$ *or* 5 *and* $G = \mathrm{GU}_1(q).2$*;*

7. $G \in \mathcal{C}_6$, $q = 5$ *or* 7 *and* $G = 2_-^{1+2}\Omega_2^-(2)$. *There is one conjugacy class of such subgroups when $q = 5$ and two conjugacy classes when $q = 7$;*

8. $G \in \mathcal{C}_6$, $q = 7$ *or* 9 *and* $G = 2_-^{1+2}\mathrm{GO}_2^-(2)$. *There are two conjugacy classes in each case; or*

9. $G \in \mathcal{S}$, $q = 11$, *and* $G = \mathrm{SL}_2(5)$ *of which there are two conjugacy classes.*

Proof. Suppose that G is a proper subgroup of $\mathrm{Sp}_2(q)$ containing a linear Singer cycle of $\mathrm{Sp}_2(q)$ and let $\mathfrak{A}$ be the linear Singer subgroup of $\mathrm{Sp}_2(q)$. First assume that $q \in \{2, 3, 4, 5, 7, 9, 11\}$. We use MAGMA [5] and the ATLAS [9] to determine the overgroups of $\mathfrak{A}$ in these cases.

If $q = 2$, then $\mathfrak{A}$ is the trivial group. Therefore all subgroups of $\mathrm{Sp}_2(2)$ contain it. Therefore G is conjugate to $\mathrm{GL}_1(2)$, $\mathrm{GU}_1(2)$ or $2 : \mathrm{GL}_1(2) \cong \mathrm{GO}_2^+(2)$.

If $q = 3$, then the linear Singer cycle of $\mathrm{Sp}_2(3)$ is the unique element of order 2 in $\mathrm{Sp}_2(3)$. Hence, it is contained in all even order subgroups. Therefore G is conjugate to one of $\mathrm{GL}_1(3)$, $3 : \mathrm{GL}_1(3)$, $\mathrm{GL}_1(3).2$, or $\mathrm{GU}_1(3).2$.

If $q = 4$, then $\mathfrak{A}$ has order 3. Moreover all subgroups of order 3 are conjugate in $\mathrm{Sp}_2(4)$. Therefore G is conjugate to any subgroup of $\mathrm{Sp}_2(4)$ whose order is divisible by 3. Up to conjugacy, these are $\mathrm{GL}_1(4)$, $4 : \mathrm{GL}_1(4)$ and $\mathrm{GO}_2^+(4)$.

If $q = 5$, then $\mathfrak{A}$ is a subgroup of order 4 and all cyclic subgroups of such order are conjugate in $\mathrm{Sp}_2(5)$. Therefore G is conjugate to any subgroup of $\mathrm{Sp}_2(5)$ that contains an element of order 4. Up to conjugacy, these are $\mathrm{GL}_1(5)$, $5 : \mathrm{GL}_1(5)$, $\mathrm{GL}_1(5).2$, $\mathrm{GU}_1(5).2$ and $2_-^{1+2}.\Omega_2^-(2)$.

If $q = 7$, then in $\mathrm{Sp}_2(7)$, $\mathfrak{A}$ has order 6 and all cyclic subgroups of such order are conjugate in $\mathrm{Sp}_2(7)$. Hence G is conjugate to any subgroup of $\mathrm{Sp}_2(7)$ containing an element of order 6. Up to conjugacy, these are $\mathrm{GL}_1(7)$, $7 : \mathrm{GL}_1(7)$, $\mathrm{GL}_1(7).2$, two conjugacy classes of $2_-^{1+2}.\Omega_2^-(2)$ and two conjugacy classes of $2_-^{1+2}.\mathrm{GO}_2^-(2)$.

If $q = 9$, then $\mathfrak{A}$ has order 8. Also all cyclic subgroups of order 8 are conjugate in $\mathrm{Sp}_2(9)$. This means G is conjugate to any subgroup of $\mathrm{Sp}_2(9)$ that contains an element of order 8. These are $\mathrm{GL}_1(9)$, $9 : \mathrm{GL}_1(9)$, $\mathrm{GL}_1(9).2$ and two conjugacy classes of $2_-^{1+2}.\mathrm{GO}_2^-(2)$, up to conjugacy.

If $q = 11$, then in $\mathrm{Sp}_2(11)$, $\mathfrak{A}$ has order 10. Since all cyclic subgroups of order 10 are conjugate in $\mathrm{Sp}_2(11)$, G is conjugate to any subgroup of $\mathrm{Sp}_2(11)$ that contains an element of order 10. Up to conjugacy, these are $\mathrm{GL}_1(11)$, $11:\mathrm{GL}_1(11)$, $\mathrm{GL}_1(11).2$ and two conjugacy classes of $\mathrm{SL}_2(5)$.

Hence, we can assume that $q \notin \{2, 3, 4, 5, 7, 9, 11\}$. The image of $\mathfrak{A}$ in $\mathrm{PSp}_2(q)$ has order $(q-1)/d$, where $d = \gcd(2, q-1)$. Since $\mathrm{PSp}_2(q) \cong \mathrm{PSL}_2(q)$, we use Theorem 2.4.1 to see which maximal subgroups of $\mathrm{PSp}_2(q)$ can contain an element of this order.

If $\mathrm{D}_{2(q+1)/d}$ contained an element of order $(q-1)/d$, then $(q-1)/d$ divides

$$\frac{2d(q+1)}{d} - \frac{2d(q-1)}{d} = 4,$$

and hence $q = 2$, 3, 5, or 9, a contradiction. The subgroups $\mathrm{D}_{2(q-1)/d}$ and $q:(q-1)/d$ clearly contain an element of order $(q-1)/d$. If $q \notin \{2, 3, 4, 5, 7, 9, 11\}$, then $(q-1)/d \geqslant 6$, so there is no element of order $(q-1)/d$ in A_4, S_4 or A_5. Lastly, let $q_0^m = q$ with m a prime. If $\mathrm{PSL}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$ contained an element of order $(q-1)/d$, then by Theorem 2.4.1, we have

$$(q_0^m - 1)/d \leqslant \begin{cases} q_0 + 1, & \text{if } q_0 \neq 4, \\ 6, & \text{if } q_0 = 4, \end{cases}$$

which gives $(m, q_0) = (2, 2)$ or $(2, 3)$. But then $q = 4$ or 9, which is a contradiction.

Therefore, since there is a single conjugacy class of cyclic subgroups of order $(q-1)/d$ in $\mathrm{PSL}_2(q)$ by [23, Theorem 2.1], we have shown that the image of $\mathfrak{A}$ is contained in $\mathrm{D}_{2(q-1)/d}$ or $q:(q-1)/d$. Let M be the preimage of $\mathrm{D}_{2(q-1)/d}$ in $\mathrm{Sp}_2(q)$. If q is even then $M = \mathrm{D}_{2(q-1)} \cong \mathrm{GO}_2^+(q)$. Since $\mathfrak{A}$ has index 2 in M, we observe G is conjugate to $\mathrm{GL}_1(q)$ or $\mathrm{GO}_2^+(q)$.

So assume that q is odd. The image of $\mathfrak{A}$ in $\mathrm{PSp}_2(q)$ is normal in $\mathrm{D}_{2(q-1)/d}$, hence

$\mathfrak{A} \trianglelefteq M$. By Proposition 3.3.1, we therefore have

$$M \leqslant \mathrm{N}_{\mathrm{Sp}_2(q)}(\mathfrak{A}) = \mathrm{GL}_1(q).2.$$

But $|M| = d\left|\mathrm{D}_{2(q-1)/d}\right|$, so $M = \mathrm{GL}_1(q).2$. Since $\mathfrak{A}$ also has index 2 in $\mathrm{GL}_1(q).2$ we observe G is conjugate to $\mathrm{GL}_1(q)$ or $\mathrm{GL}_1(q).2$.

Therefore, let M be the preimage of $q:(q-1)/d$ in $\mathrm{Sp}_2(q)$. The image of $q:\mathrm{GL}_1(q)$ in $\mathrm{PSp}_2(q)$ has a normal p-subgroup. Moreover the only maximal subgroup of $\mathrm{PSL}_2(q)$ having a normal p-subgroup is $q:(q-1)/d$. Thus we must have $M = q:\mathrm{GL}_1(q)$. Now $\mathrm{GL}_1(q)$ acts transitively on the elements of order p in the subgroup of M of order q. Therefore the only subgroups of M that contain $\mathfrak{A}$ are $q:\mathrm{GL}_1(q)$ and $\mathrm{GL}_1(q)$. This means $G = q:\mathrm{GL}_1(q)$ or $\mathrm{GL}_1(q)$. □

Theorem 4.2.2 *Let G be a proper subgroup of $\mathrm{GU}_2(q)$ containing a linear Singer cycle of $\mathrm{GU}_2(q)$. Then up to conjugacy, G is one of the following:*

1. $\mathrm{GL}_1(q^2)$, *linear Singer subgroup;*
2. $G \in \mathcal{C}_1$ *and* $G = q:\mathrm{GL}_1(q^2)$;
3. $G \in \mathcal{C}_2$ *and* $G = \mathrm{GL}_1(q^2).2$;
4. $G \in \mathcal{C}_1$, $q = 2$ *and* $G = \mathrm{GU}_1(2) \times \mathrm{GU}_1(2)$;
5. $G \in \mathcal{C}_2$, $q = 3$ *and* $G = \mathrm{GU}_1(3) \wr \mathrm{S}_2$; *or*
6. $G \in \mathcal{C}_6$, $q = 5$ *and* $G = \mathrm{C}_6 \circ 2^{1+2}\mathrm{Sp}_2(2)$.

Proof. Let $\mathfrak{A}$ be the linear Singer subgroup of $\mathrm{GU}_2(q)$ and suppose $G \leqslant \mathrm{GU}_2(q)$ contains a linear Singer cycle of $\mathrm{GU}_2(q)$. Assume first that $q \leqslant 5$. We can again use MAGMA [5] and the ATLAS [9] to verify these cases.

If $q = 2$, then $\mathfrak{A} = \mathrm{Z}(\mathrm{GU}_2(q))$. Therefore G is one of the subgroups containing the centre of $\mathrm{GU}_2(q)$. Up to conjugacy, these are $\mathrm{GL}_1(4)$, $2 : \mathrm{GL}_1(4) \cong \mathrm{GL}_1(4).2$ and $\mathrm{GU}_1(2) \times \mathrm{GU}_1(2)$.

If $q = 3$, then $\mathfrak{A}$ has order 8 and all cyclic subgroups of such order are conjugate in $\mathrm{GU}_2(3)$. Therefore G is conjugate to any subgroup of $\mathrm{GU}_2(3)$ that contains an element of order 8. These are $\mathrm{GL}_1(9)$, $3 : \mathrm{GL}_1(9)$, $\mathrm{GL}_1(9).2$, and $\mathrm{GU}_1(3) \wr \mathrm{S}_2$.

If $q = 4$, then $\mathfrak{A}$ has order 15. Furthermore there is a single conjugacy class of subgroups of order 15 in $\mathrm{GU}_2(4)$. This means G is conjugate to any subgroup of $\mathrm{GU}_2(4)$ that contains an element of order 15. These subgroups are $\mathrm{GL}_1(16)$, $\mathrm{GL}_1(16).2$ and $4 : \mathrm{GL}_1(16)$.

If $q = 5$, then $\mathfrak{A}$ has order 24. In $\mathrm{GU}_2(5)$, all cyclic subgroups of order 24 are conjugate. Thus G is conjugate to any subgroup of $\mathrm{GU}_2(5)$ containing an element of order 24. These are $\mathrm{GL}_1(25)$, $5 : \mathrm{GL}_1(25)$, $\mathrm{GL}_1(25).2$ and $\mathrm{C}_6 \circ 2^{1+2}.\mathrm{Sp}_2(2)$.

Now suppose that $q \geqslant 7$. The image of $\mathfrak{A}$ in $\mathrm{PGU}_2(q)$ has order $q-1$. Since $\mathrm{PGU}_2(q) \cong \mathrm{PGL}_2(q)$, we can use Corollary 2.4.2, to determine the maximal subgroups of $\mathrm{PGU}_2(q)$ that contain an element of this order.

If $\mathrm{D}_{2(q+1)}$ contained an element of order $q-1$, then $q-1$ divides

$$2(q+1) - 2(q-1) = 4.$$

Hence $q = 2$, 3 or 5 contrary to our assumptions. Also, the subgroups $\mathrm{D}_{2(q-1)}$ and $q : q-1$ clearly contain elements of order $q-1$. If $q \geqslant 7$, then $q-1 \geqslant 6$. This means S_4 cannot contain an element of order $q-1$. Now if $q = q_0^m$, with m prime and $\mathrm{PGL}_2(q_0)$ contained an element of order $q-1$, then by Theorem 2.2.6, we have

$$q_0^m - 1 \leqslant \begin{cases} q_0 + 1, & \text{if } q_0 \neq 4, \\ 6, & \text{if } q_0 = 4. \end{cases}$$

We therefore have $(m, q_0) = (2,2)$ and $q = 4$, which contradicts our assumptions. Lastly, assume q is odd and $\mathrm{PSL}_2(q)$ contains an element of order $q-1$. Since $q-1$ is coprime to q, by [22, Table A.1], we have $q - 1 \leqslant (q+1)/2$. But this gives $q \leqslant 3$, a contradiction.

Therefore, since there is a single conjugacy class of cyclic subgroups of order $q-1$ in $\mathrm{PGL}_2(q)$ by [23, Theorem 2.1], we have shown that the image of $\mathfrak{A}$ in $\mathrm{PGU}_2(q)$ is contained in a conjugate of $\mathrm{D}_{2(q-1)}$ or $q : q-1$. If M is the preimage of $\mathrm{D}_{2(q-1)}$ in $\mathrm{GU}_2(q)$, then since the image of $\mathfrak{A}$ in $\mathrm{PGU}_2(q)$ is normal in $\mathrm{D}_{2(q-1)}$, we see that $\mathfrak{A} \trianglelefteq M$. By Proposition 3.3.1, we have

$$M \leqslant \mathrm{N}_{\mathrm{GU}_2(q)}(\mathfrak{A}) = \mathrm{GL}_1\left(q^2\right).2.$$

But $|M| = (q+1)\left|\mathrm{D}_{2(q-1)}\right|$, so $M = \mathrm{GL}_1(q^2).2$. Hence, if $G \leqslant \mathrm{GL}_1(q^2).2$ contains $\mathfrak{A}$, then $G = \mathrm{GL}_1(q^2)$ or $\mathrm{GL}_1(q^2).2$.

Therefore, let M be the preimage of $q : q-1$ in $\mathrm{GU}_2(q)$. The image of $q : \mathrm{GL}_1(q^2)$ in $\mathrm{PGU}_2(q)$ has a normal p-subgroup. Since the only maximal subgroup of $\mathrm{PGL}_2(q)$ having a normal p-subgroup is $q : q-1$, we must have $M = q : \mathrm{GL}_1(q^2)$. Now $\mathrm{GL}_1(q^2)$ acts transitively on the elements of order p in the subgroup of M of order q. Therefore. the only subgroups of M that contain $\mathfrak{A}$ are $q : \mathrm{GL}_1(q^2)$ and $\mathrm{GL}_1(q^2)$. Therefore either $G = q : \mathrm{GL}_1(q^2)$ or $\mathrm{GL}_1(q^2)$. □

4.3 Four-dimensional orthogonal groups

We finish this chapter by turning our attention to the case when $X = \mathrm{GO}_4^+(q)$. It is well known that $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$, see for example [24, Proposition 2.9.1]. Therefore we shall need to know about subgroups of direct products of simple groups in our analysis. We start with a general result about the maximal subgroups of such groups. We adapt the method of [32].

Proposition 4.3.1 *Let M be a maximal subgroup of $G := L \times R$ where L and R are isomorphic non-abelian simple groups. Then one of the following holds:*

1. *$M = L \times M_R$, where M_R is a maximal subgroup of R;*

2. *$M = M_L \times R$, where M_L is a maximal subgroup of L; or*

3. *$M = \Delta_\theta := \{(a, a\theta) : a \in L\}$, where $\theta : L \to R$ is an isomorphism and $M \cong L \cong R$.*

Proof. Let $\pi_L : G \to R$ and $\pi_R : G \to R$ be the projection maps defined by $(l, r)\,\pi_L = (l, 1)$ and $(l, r)\,\pi_R = (1, r)$. Set $M_L = (M)\,\pi_L$ and $M_R = (M)\,\pi_R$. Note that if $(l, r) \in M$, then $(l, r) = (l, 1)\,(1, r) \in M_L M_R$, so $M \leqslant M_L M_R \leqslant G$. But M is maximal, so either $M = M_L M_R$ or $M_L M_R = G$.

If $M = M_L M_R$, then note that

$$M = M_L M_R \leqslant M_L \times R \leqslant G$$

and

$$M = M_L M_R \leqslant L \times M_R \leqslant G,$$

so either $M = M_L \times R$ or $M = L \times M_R$. In these cases, M_L and M_R are proper subgroups of L and R, respectively and π_L and π_R are surjective homomorphisms. Therefore M_L and M_R are maximal subgroups of L and R, respectively.

So suppose that $G = M_L M_R$. Then $M_L = L$ and $M_R = R$. Since $L \trianglelefteq G$, we have $M \cap L \trianglelefteq M$, hence

$$M \cap L = (M \cap L)\,\pi_L \trianglelefteq (M)\,\pi_L = M_L = L.$$

If $M \cap L = L$, then by the First Isomorphism Theorem, we have

$$M/L \cong (M)\,\pi_R = R,$$

so $|M| = |L|\,|R| = |G|$, contrary to $M \neq G$. Therefore since L is simple, we must have $M \cap L = 1$. By a similar argument, $M \cap R = 1$.

Now, given $(x, y) \in M$, define the map $\theta : L \to R$ by $x\theta = y$. If $(x, y), (x, y') \in M$, then

$$(x, y)^{-1}(x, y') = \left(1, y^{-1}y'\right) \in M \cap R = 1,$$

so $y = y'$, which means that θ is well defined. We also have

$$(xx')\,\theta = yy' = (x\theta)\,(x'\theta)\,,$$

so θ is a homomorphism. Also, reversing the roles of x and y, the map $\phi : R \to L$ defined by $y\phi = x$ is an inverse to θ, so θ is an isomorphism from L to R. Now define the group

$$\Delta_\theta := \{(x, x\theta) : x \in L\} < G.$$

Then if $(x, y) \in M$, we have $x\theta = y$, so $(x, y) \in \Delta_\theta$. By the maximality of M, we conclude that $M = \Delta_\theta$. It is clear that $\Delta_\theta \cong L \cong R$. $\square$

The next result gives the conjugacy of maximal subgroups of direct products of simple groups.

Proposition 4.3.2 *Let G, L and R be as in Proposition 4.3.1. Two maximal subgroups $L \times M_1$ and $L \times M_2$ of G are conjugate in G if and only if M_1 and M_2 are conjugate in R. Similarly, two maximal subgroups $M_1 \times R$ and $M_2 \times R$ of G are conjugate in G if and only if M_1 and M_2 are conjugate in L.*

Also, two maximal subgroups Δ_θ and Δ_ϕ are conjugate in G if and only if $\theta^{-1}\phi$ is an inner automorphism of R.

Proof. Let $(x, y) \in G$ such that $(L \times M_1)^{(x,y)} = L \times M_2$. Then

$$(L \times M_1)^{(x,y)} = L^x \times M_1^y = L \times M_1^y.$$

Hence $M_1^y = M_2$.

Conversely, let $y \in R$ such that $M_1^y = M_2$. Then

$$(L \times M_1)^{(1,y)} = L \times M_1^y = L \times M_2,$$

as required. The proof of the second statement is similar.

Now, $(x, y) \in G$ such that $\Delta_\theta^{(x,y)} = \Delta_\phi$. Then for all $(w, w\phi)) \in \Delta_\phi$, we have

$$(w, w\phi)) = (z, z\theta)^{(x,y)} = (z^x, (z\theta)^y),$$

for some z. Hence

$$w\phi = (z\theta)^y = \left(\left(w^{x^{-1}}\right)\theta\right)^y = (w\theta)^{(x\theta)^{-1}y}.$$

Therefore letting $g = (x\theta)^{-1} y$ and $c_g : R \to R$ be conjugation by g, we see $\phi = \theta c_g$, so $\theta^{-1}\phi = c_g$.

Conversely suppose that $\theta^{-1}\phi = c_g$, for some g. Then if $(x, x\phi) \in \Delta_\phi$, then

$$(x, x\phi) = (x, (x\theta)\, c_g) = (x, x\theta)^{(1,g)} \in \Delta_\theta^{(1,g)}.$$

On the other hand, if $(x, x\theta) \in \Delta_\theta$, then

$$(x, x\theta)^{(1,g)} = (x, (x\theta)\, c_g) = (x, x\phi) \in \Delta_\phi.$$

Therefore $\Delta_\theta^{(1,g)} = \Delta_\phi$, as required. $\square$

As an aside, we can deduce the number of conjugacy classes of the Δ_θ.

Corollary 4.3.3 *The number of conjugacy classes of maximal subgroups of the form Δ_θ is $|\mathrm{Out}\,(R)|$.*

Proof. The conjugacy classes of such subgroups partition the set of all Δ_θ. By Proposition 4.3.2, the size of each conjugacy class is $|\mathrm{Inn}\,(R)|$. Therefore, if there are r conjugacy classes, we have $r\,|\mathrm{Inn}\,(R)| = |\mathrm{Aut}\,(R)|$, so $r = |\mathrm{Aut}\,(R)| \,/\, |\mathrm{Inn}\,(R)| = |\mathrm{Out}\,(R)|$. $\square$

Let $\mathfrak{A}$ be the linear Singer subgroup of $\mathrm{GO}_{2n}^{+}(q)$ and $\overline{\mathfrak{A}}$ be the image of $\mathfrak{A}$ in $\mathrm{PGO}_4^{+}(q)$. We wish to know the order of $\overline{\mathfrak{A}} \cap \mathrm{P}\Omega_4^{+}(q)$. It follows from the definition of a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$ in Definition 3.1.2, that $\mathfrak{A}$ lies in $\mathrm{SO}_4^{+}(q)$. The following lemma gives a necessary and suffient condition for $\mathfrak{A}$ to lie in $\Omega_4^{+}(q)$. From this we can deduce $\left|\overline{\mathfrak{A}} \cap \mathrm{P}\Omega_4^{+}(q)\right|$.

Lemma 4.3.4 *The linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$ lies in $\Omega_{2n}^{+}(q)$ if and only if q is even.*

Proof. If q is even, then $q^n - 1$ is odd. Since $\Omega_{2n}^{+}(q)$ has index 2 in $\mathrm{GO}_{2n}^{+}(q)$, the linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$ lies in $\Omega_{2n}^{+}(q)$.

Conversely, suppose that q is odd. Let $v_1, \ldots, v_n, w_1, \ldots, w_n$ be the basis of the underlying vector space as in Proposition 2.3.1. If a is a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$, then a fixes the subspaces $W := \langle v_1, \ldots, v_n \rangle$ and $U := \langle w_1, \ldots, w_n \rangle$. If $a \in \Omega_{2n}^{+}(q)$, then by [24, Lemma 2.7.2], the determinant of a considered as a linear map of W, $\det_W(a)$ is a square. Since q is odd, $\det_W(a)$ lies inside the index 2 subgroup of $\mathrm{GF}(q)^\times$. But by [7, the proof of Lemma 4.2], $\det_W(a)$ generates $\mathrm{GF}(q)^\times$, a contradiction. Therefore a does not lie in $\Omega_{2n}^{+}(q)$. $\square$

Now, if q is even, then $\left|\mathrm{Z}\left(\Omega_4^{+}(q)\right)\right| = 1$ and so by Lemma 4.3.4, $\left|\overline{\mathfrak{A}} \cap \mathrm{P}\Omega_4^{+}(q)\right| = q^2 - 1$.

If q is odd, then by the Second Isomorphism Theorem and Lemma 4.3.4, we have

$$|\mathfrak{A}| / \left|\mathfrak{A} \cap \Omega_4^+(q)\right| = \left|\mathfrak{A}\Omega_4^+(q)\right| / \left|\Omega_4^+(q)\right| = \left|\mathrm{SO}_4^+(q)\right| / \left|\Omega_4^+(q)\right| = 2.$$

Hence $\left|\mathfrak{A} \cap \Omega_4^+(q)\right| = (q^2-1)/2$ and since $\left|\mathrm{Z}\left(\Omega_4^+(q)\right)\right| = 2$, we have $\left|\overline{\mathfrak{A}} \cap \mathrm{P}\Omega_4^+(q)\right| = (q^2-1)/4$.

Before we prove the result for $X = \mathrm{GO}_4^+(q)$, we shall need the following lemma.

Lemma 4.3.5 *Let* $q \notin \{2, 3, 4, 5, 7, 9, 11\}$ *and let* M *be a maximal subgroup of* $\mathrm{PSL}_2(q)$. *Also let* $d = \gcd(2, q-1)$.

1. *If* M *contains an element of order* $(q-1)/d$, *then either* $M = q : (q-1)/d$ *or* $\mathrm{D}_{2(q-1)/d}$.

2. *If* M *contains an element of order* $(q+1)/d$, *then* $M = \mathrm{D}_{2(q+1)/d}$.

Proof.

1. This follows from the proof of Theorem 4.2.1.

2. We use Theorem 2.4.1 to determine which maximal subgroups of $\mathrm{PSL}_2(q)$ contain an element of order $(q+1)/d$.

   If $\mathrm{D}_{2(q-1)/d}$ contains an element of order $(q+1)/d$, then $(q+1)/d$ divides

   $$\frac{2d(q+1)}{d} - \frac{2d(q-1)}{d} = 4.$$

   Hence $q = 3$ or 7, contrary to our assumptions. Similarly, if $q : (q-1)/d$ contains an element of order $(q+1)/d$, then $(q+1)/d$ divides

   $$\frac{dq(q-1)}{d} - \frac{d(q-2)(q+1)}{d} = 2.$$

   So $q = 3$, which cannot happen. Now if $q \notin \{2, 3, 4, 5, 7, 9, 11\}$, then $(q+1)/d \geqslant 7$, so A_4, S_4 and A_5 cannot contain an element of order $(q+1)/d$. Let $q = q_0^m$ where

m is a prime. If $\mathrm{PSL}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$ contain an element of order $(q+1)/d$, then by Theorem 2.2.6, we have

$$(q_0^m+1)/d \leqslant \begin{cases} q_0+1, & \text{if } q_0 \neq 4, \\ 6, & \text{if } q_0 = 4, \end{cases}$$

which gives $(m, q_0) = (2, 2)$ or $(2, 3)$. But then $q = 4$ or 9.

Since $\mathrm{D}_{2(q+1)/d}$ contains an element of order $(q+1)/d$ and we have exhausted all other possibilities for M, the result follows. □

We are now in a position to prove the case when $X = \mathrm{GO}_4^+(q)$.

Theorem 4.3.6 *Suppose G is a subgroup of $\mathrm{GO}_4^+(q)$ not containing $\Omega_4^+(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GO}_4^+(q)$. Then one of the following holds:*

1. *$G \in \mathcal{C}_1$ and G is contained in $q : \mathrm{GL}_2(q)$;*

2. *$G \in \mathcal{C}_2$ and G is contained in $\mathrm{GL}_2(q).2$;*

3. *$G \in \mathcal{C}_3$ and G is contained in $\mathrm{GU}_2(q).2$;*

4. *$q = 2$ and G is contained in $\left(\Omega_2^-(2) \times \Omega_2^-(2)\right) : 4$;*

5. *$q = 3$, $G \in \mathcal{C}_2$ and G is contained one of two conjugates of $\mathrm{GO}_1(3) \wr \mathrm{S}_4$; or*

6. *$q = 5$ and G is contained in $2.(\mathrm{A}_5 \times \mathrm{A}_4).2$.*

Proof. Let $\mathfrak{A}$ be the Singer subgroup of $\mathrm{GO}_4^+(q)$, and suppose G is a subgroup of $\mathrm{GO}_4^+(q)$ not containing $\Omega_4^+(q)$ that contains a linear Singer cycle of $\mathrm{GO}_4^+(q)$. First assume $q \in \{2, 3, 4, 5, 7, 9, 11\}$. As in Section 4.2, we use MAGMA [5] to give the result in these cases.

If $q = 2$, then $\mathfrak{A}$ has order 3, so is contained in a Sylow 3-subgroup of $\mathrm{GO}_4^+(2)$. Also all maximal subgroups of $\mathrm{GO}_4^+(2)$ contain a Sylow 3-subgroup. Therefore up to conjugacy, G is contained in $\left(\Omega_2^-(2) \times \Omega_2^-(2)\right).4$ and one of two conjugacy classes of groups isomorphic to $\mathrm{GU}_2(2).2$.

If $q = 3$, then $\mathfrak{A}$ has order 8 and there is a single conjugacy class of cyclic subgroups of order 8 in $\mathrm{GO}_4^+(3)$. This means G is contained in a subgroup containing an element of order 8. The maximal subgroups of $\mathrm{GO}_4^+(3)$ that contains such an element are $\mathrm{SO}_4^+(3)$ and two conjugacy classes of groups isomorphic to $\mathrm{GO}_1(3) \wr \mathrm{S}_4$. The maximal subgroups of $\mathrm{SO}_4^+(3)$ that contain an element of order 8 are $3 : \mathrm{GL}_2(3)$, $\mathrm{GU}_2(3).2$ and two conjugacy classes of groups which consist of the elements of $\mathrm{GO}_1(3) \wr \mathrm{S}_4$ having determinant 1. Therefore, up to conjugacy, G is contained in $3 : \mathrm{GL}_2(3)$, $\mathrm{GU}_2(3).2$ or one of the two classes of groups isomorphic to $\mathrm{GO}_1(3) \wr \mathrm{S}_4$.

If $q = 4$, then $\mathfrak{A}$ has order 15 and there is a single conjugacy class of subgroups of order 15 in $\mathrm{GO}_4^+(4)$, so G is contained in a subgroup containing an element of order 15. The only maximal subgroup of $\mathrm{GO}_4^+(4)$ that contains such an element is $\Omega_4^+(4)$, whereas the maximal subgroups of $\Omega_4^+(4)$ that contain an element of order 15 are $4 : \mathrm{GL}_2(4)$, $\mathrm{GL}_2(4).2$ and $\mathrm{GU}_2(4).2$. Therefore G is contained in a conjugate of $4 : \mathrm{GL}_2(4)$, $\mathrm{GL}_2(4).2$ or $\mathrm{GU}_2(4).2$.

If $q = 5$, then $\mathfrak{A}$ has order 24 and there is a single conjugacy class of cyclic subgroups of order 24 in $\mathrm{GO}_4^+(5)$. Thus G is contained in a subgroup containing an element of order 24. But the only maximal subgroup of $\mathrm{GO}_4^+(5)$ that contains such an element is $\mathrm{SO}_4^+(5)$, and the maximal subgroups of $\mathrm{SO}_4^+(5)$ that contain an element of order 24 are $5 : \mathrm{GL}_2(5)$, $\mathrm{GU}_2(5).2$ and $2.(\mathrm{A}_5 \times \mathrm{A}_4).2$. Therefore G is contained in a conjugate of $5 : \mathrm{GL}_2(5)$, $\mathrm{GU}_2(5).2$ or $2.(\mathrm{A}_5 \times \mathrm{A}_4).2$.

If $q = 7$, 9 or 11, then $\mathfrak{A}$ has order 48, 80 or 120, respectively. For these values of q, there is a single conjugacy class of cyclic subgroups of order $q^2 - 1$ in $\mathrm{GO}_4^+(q)$, so G is contained in a subgroup containing an element of order q^2-1. The only maximal subgroup of $\mathrm{GO}_4^+(q)$ that contains such an element is $\mathrm{SO}_4^+(q)$, whereas the maximal subgroups of $\mathrm{SO}_4^+(q)$ that contain an element of order q^2-1 are $q:\mathrm{GL}_2(q)$, $\mathrm{GL}_2(q).2$ and $\mathrm{GU}_2(q).2$. Therefore G is contained in a conjugate of $q:\mathrm{GL}_2(q)$, $\mathrm{GL}_2(q).2$ or $\mathrm{GU}_2(q).2$.

Therefore we may assume that $q \notin \{2, 3, 4, 5, 7, 9, 11\}$. Let $L = \mathrm{PSL}_2(q) \times 1$ and $R = 1 \times \mathrm{PSL}_2(q)$, so $\mathrm{P\Omega}_4^+(q) \cong L \times R$. As mentioned above $\overline{\mathfrak{A}} \cap \mathrm{P\Omega}_4^+(q)$ has order $(q^2-1)/d^2$, where $d = \gcd(2, q-1)$. If $\mathrm{PSL}_2(q)$ contains an element of this order, then by Theorem 2.2.6, we have

$$(q^2-1)/d^2 \leqslant \begin{cases} q+1, & \text{if } q \neq 4, \\ 6, & \text{if } q = 4, \end{cases}$$

which gives $q = 2$, 3 or 5, a contradiction.

Hence, if M is a maximal subgroup of $\mathrm{P\Omega}_4^+(q)$ containing $\overline{\mathfrak{A}} \cap \mathrm{P\Omega}_4^+(q)$, then by Proposition 4.3.1, either $M = L \times M_R$, where M_R is a maximal subgroup of R, or $M = M_L \times R$, where M_L is a maximal subgroup of L.

Consider $\overline{\mathfrak{A}} \cap M_R$. By [22], the two largest element orders coprime to q are $(q-1)/d$ and $(q+1)/d$. Therefore as

$$\frac{(q^2-1)}{d^2} = \frac{(q-1)}{d} \cdot \frac{(q+1)}{d},$$

the order of $\overline{\mathfrak{A}} \cap M_R$ is either $(q-1)/d$ or $(q+1)/d$. Therefore by Lemma 4.3.5, M_R is one of $q:(q-1)/d$, $\mathrm{D}_{2(q-1)/d}$ or $\mathrm{D}_{2(q+1)/d}$.

For simplicity, let

$$K := \begin{cases} \mathrm{SO}_4^+(q), & \text{if } q \text{ is odd}, \\ \Omega_4^+(q) & \text{if } q \text{ is even} \end{cases}$$

and let $\overline{K}$ be the image of K in $\mathrm{PGO}_4^+(q)$. By [24, Lemma 2.9.4, Lemma 2.5.8], $\mathrm{PGO}_4^+(q)$

acts on $\{L, R\}$ by conjugation and there is an element $g \in \mathrm{PGO}_4^+(q)/\overline{K}$ such that $L^g = R$. Hence, if N is a maximal subgroup of $\mathrm{PSL}_2(q)$, then $L \times N$ is conjugate in $\mathrm{PGO}_4^+(q)$ to $N \times R$. This means up to conjugacy in $\mathrm{PGO}_4^+(q)$, M is one of

1. $L \times q : (q-1)/d$,
2. $L \times \mathrm{D}_{2(q-1)/d}$ or
3. $L \times \mathrm{D}_{2(q+1)/d}$.

Now let $\overline{G}$ be the image of G in $\mathrm{PGO}_4^+(q)$. We will show that $G \leqslant K$.

Consider $\overline{G} \cap \mathrm{P}\Omega_4^+(q)$. This contains an element of order $(q^2-1)/d^2$ and so lies in $L \times M_R$, where M_R is one of $q : (q-1)/d$, $\mathrm{D}_{2(q-1)/d}$ or $\mathrm{D}_{2(q+1)/d}$, as shown above.

As $\overline{G} \cap \mathrm{P}\Omega_4^+(q)$ contains an element of order $(q^2-1)/d^2$, there exists a prime r such that $\overline{G} \cap \mathrm{P}\Omega_4^+(q)$ contains a Sylow r-subgroup of L. For example, we can take r to be a prime dividing

$$\begin{cases} (q-1)/d, & \text{if } M_R = \mathrm{D}_{2(q+1)/d}, \\ (q+1)/d, & \text{otherwise.} \end{cases}$$

Let T be such a Sylow subgroup of $\overline{G} \cap \mathrm{P}\Omega_4^+(q)$. We know $\overline{G} \cap \mathrm{P}\Omega_4^+(q) \trianglelefteq \overline{G}$, so by the Frattini argument, we have $\overline{G} = \mathrm{N}_{\overline{G}}(T)\left(\overline{G} \cap \mathrm{P}\Omega_4^+(q)\right)$.

Suppose $\overline{G}$ is not contained in $\overline{K}$. Then there is $g \in \overline{G}$ such that $L^g = R$. In particular, we may pick $n \in \mathrm{N}_{\overline{G}}(T)$ such that $L^n = R$. But this means

$$T = T \cap T = T \cap T^n \leqslant L \cap L^n = L \cap R = 1,$$

which cannot happen. Hence $\overline{G} \leqslant \overline{K}$ and so $G \leqslant K$.

Finally, let Y be one of $q : \mathrm{GL}_2(q)$, $\mathrm{GL}_2(q).2$ or $\mathrm{GU}_2(q).2$ and let $\overline{Y}$ be the image of Y in $\mathrm{PGO}_4^+(q)$. The same arguments in Theorems 5.1.1, 5.2.5 and Proposition 5.3.8 applied to $\mathrm{GO}_4^+(q)$ show that Y contains a linear Singer cycle of $\mathrm{GO}_4^+(q)$, so the above argument says that $Y \leqslant K$. This means $\overline{Y} \cap \mathrm{P}\Omega_4^+(q)$ has order $|Y|/d^2$. Also $\overline{Y} \cap \mathrm{P}\Omega_4^+(q)$ contains $\overline{\mathfrak{A}} \cap \mathrm{P}\Omega_4^+(q)$ and so is contained in a conjugate of $L \times M_R$.

If $Y = q : \mathrm{GL}_2(q)$, then $\left|\overline{Y} \cap \mathrm{P}\Omega_4^+(q)\right| = q^2(q-1)(q^2-1)/d^2$. By comparing orders, we observe $\overline{Y} \cap \mathrm{P}\Omega_4^+(q)$ is conjugate to $L \times q : (q-1)/d$.

If $Y = \mathrm{GL}_2(q).2$, then $\left|\overline{Y} \cap \mathrm{P}\Omega_4^+(q)\right| = 2q(q-1)(q^2-1)/d^2$. Again by comparing orders, we see $\overline{Y} \cap \mathrm{P}\Omega_4^+(q)$ is conjugate to $L \times \mathrm{D}_{2(q-1)/d}$.

If $Y = \mathrm{GU}_2(q).2$, then $\left|\overline{Y} \cap \mathrm{P}\Omega_4^+(q)\right| = 2q(q+1)(q^2-1)/d^2$ and so by comparing orders, $\overline{Y} \cap \mathrm{P}\Omega_4^+(q)$ is conjugate to $L \times \mathrm{D}_{2(q+1)/d}$.

We have shown that if $G \leqslant \mathrm{GO}_4^+(q)$ containing a linear Singer cycle of $\mathrm{GO}_4^+(q)$, then the image of G in $\mathrm{P}\Omega_4^+(q)$ is contained in $L \times M_R$. Since $G \leqslant K$ and the $L \times M_R$ form a complete list of maximal subgroups of $\mathrm{P}\Omega_4^+(q)$ containing an element of order $(q^2-1)/d^2$, we conclude that G is contained in a conjugate of $q : \mathrm{GL}_2(q)$, $\mathrm{GL}_2(q).2$ or $\mathrm{GU}_2(q).2$. $\square$

Chapter 5

Geometric subgroups containing a linear Singer cycle

In this chapter, we begin the proof of the main theorem. Let X be one of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ or $\mathrm{GO}_{2n}^{+}(q)$, where $n \geqslant 2$ for $\mathrm{Sp}_{2n}(q)$ and $\mathrm{GU}_{2n}(q)$ and $n \geqslant 3$ for $\mathrm{GO}_{2n}^{+}(q)$, and suppose that $G \leqslant X$ contains a linear Singer cycle of X. Our main tool will be Aschbacher's classification of the subgroups of X, into the so called Aschbacher classes, given in [2].

We first assume that G lies in one of the classes $\mathcal{C}_1$ to $\mathcal{C}_8$ of Aschbacher's theorem. We will use the subgroup lists in Tables 2.2, 2.3 and 2.4 to determine which classes of subgroups that G can lie in. Most of the time, we will use primitive prime divisors of $q^{un}-1$ as well as bounds on the element orders in classical groups found in [14] and [28]. As before, let $\mathfrak{A}$ denote the linear Singer subgroup of X.

5.1 Reducible subgroups

Suppose first that G acts reducibly on V, so G stabilizes a proper, non-trivial subspace of V, so lies in class $\mathcal{C}_1$. Assume first that $X \neq \mathrm{Sp}_4(2)$. The following theorem immediately follows from Theorem 3.2.2. Recall that $V = W_1 \oplus W_2$, where

$$W_1 = \{(v, 0) : v \in \mathrm{GF}(q^{un})\},$$

and

$$W_2 = \{(0, \theta^\alpha) : \theta \in (\mathrm{GF}(q^{un}))^{*\alpha}\}.$$

Theorem 5.1.1 *Let $G \leqslant X$ contain a linear Singer cycle of X and suppose that G is reducible. Also, let W_1 and W_2 be the subspaces of V defined above. If $X \neq \mathrm{Sp}_4(2)$, then either $G \leqslant \mathrm{Stab}_X(W_1)$ or $G \leqslant \mathrm{Stab}_X(W_2)$.*

The subspaces W_1 and W_2 are n-dimensional and isotropic and so their stabilizers are maximal parabolic subgroups of X. From Tables 2.2, 2.3 and 2.4, if M is the stabilizer of one of these subspaces in X, then

$$M \cong \begin{cases} q^{n(n+1)/2} : \mathrm{GL}_n(q), & \text{if } X = \mathrm{Sp}_{2n}(q), \\ q^{n^2} : \mathrm{GL}_n(q^2), & \text{if } X = \mathrm{GU}_{2n}(q), \\ q^{n(n-1)/2} : \mathrm{GL}_n(q), & \text{if } X = \mathrm{GO}^+_{2n}(q). \end{cases}$$

Now assume that $X = \mathrm{Sp}_4(2)$. Recall the definitions of the subspaces U_1, U_ω and U_{ω^2} of V from Theorem 3.2.2. These, together with W_1 and W_2, are the only subspaces invariant under the action of the linear Singer cycle. Hence in this case, we obtain the following.

Theorem 5.1.2 *Suppose that $X = \mathrm{Sp}_4(2)$. Let $G \leqslant X$ contain a linear Singer cycle of X and suppose that G is reducible. Then G lies in the stabilizer of one of W_1, W_2, U_1, U_ω or U_{ω^2}.*

Each of the subspaces W_1, W_2 and U_ω are 2-dimensional isotropic subspaces. Therefore their stabilizers are maximal parabolic subgroups isomorphic to

$$2^{2(2+1)/2} : \mathrm{GL}_2(2) \cong 2^3 : \mathrm{S}_3 \cong 2 \wr \mathrm{S}_3.$$

On the other hand, the subspaces U_1 and U_{ω^2} are 2-dimensional non-degenerate subspaces and $U_1^\perp = U_{\omega^2}$. This means their stabilizer is isomorphic to

$$\mathrm{Sp}_2(2) \times \mathrm{Sp}_2(2) \cong \mathrm{S}_3 \times \mathrm{S}_3.$$

This group is not maximal in X since it is contained in the direct sum stabilizer $\mathrm{Sp}_2(2) \wr 2$ which is a member of $\mathcal{C}_2$. We shall deal with this in the next section.

5.2 Imprimitive subgroups

Suppose that G acts irreducibly on V and assume that G acts imprimitively on V. That is, G preserves a direct sum decomposition $V = \bigoplus_{i=1}^{m} V_i$, where the V_i are subspaces having the same dimension. We investigate when the linear Singer cycle of X can preserve such a decomposition. The case when the V_i are isotropic subspaces follows from Theorem 3.2.2. When the V_i are non-degenerate, we use primitive prime divisors of $q^{un} - 1$ to obtain conditions on m. We then apply element order bounds from Theorem 2.2.6. From now on, we consider the symplectic, unitary and orthogonal cases separately.

Symplectic Case

Let $X = \mathrm{Sp}_{2n}(q)$. Our Theorem in this section is the following.

Theorem 5.2.1 *Let $G \leqslant \mathrm{Sp}_{2n}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. Also assume that G preserves a direct sum decomposition of V, so G lies in class $\mathcal{C}_2$. Then either q is odd and G is contained in $\mathrm{GL}_n(q).2$ or $(n, q) = (2, 2)$ or $(2, 3)$*

and G lies in $\mathrm{Sp}_2(q) \wr \mathrm{S}_2$.

It follows directly from Theorem 3.2.2 that a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$ preserves the isotropic direct sum $W_1 \oplus W_2$, and so lies in the isotropic direct sum stabilizer $\mathrm{GL}_n(q).2$. Therefore we only need to consider the case when each V_i is non-degenerate in which case the stabilizer of the direct sum is $\mathrm{Sp}_{2k}(q) \wr \mathrm{S}_m$ with $n = km$.

Proposition 5.2.2 *Let M be the subgroup* $\mathrm{Sp}_{2k}(q) \wr \mathrm{S}_m$ *of* $\mathrm{Sp}_{2n}(q)$*, with $km = n$. Then M contains a linear Singer cycle of* $\mathrm{Sp}_{2n}(q)$ *if and only if $(k, m) = (1, 2)$ and $q = 2$ or 3.*

Proof. Let $M = \mathrm{Sp}_{2k}(q) \wr \mathrm{S}_m$ and suppose first that $m \neq 2$. If a primitive prime divisor of $q^n - 1$ does not exist, then by our assumptions, we have $(q, n) = (2, 6)$ and either $(k, m) = (1, 6)$ or $(2, 3)$. But in these cases, 7 divides the order of $\mathfrak{A}$, but does not divide the orders of $\mathrm{Sp}_2(2) \wr \mathrm{S}_6$ or $\mathrm{Sp}_4(2) \wr \mathrm{S}_3$.

Therefore, $q^n - 1$ has a primitive prime divisor, r. Since

$$r \geqslant n + 1 = km + 1 > m,$$

r cannot divide $|\mathrm{S}_m|$ and so divides $|\mathrm{Sp}_{2k}(q)|$. This means that r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant k$. This is a contradiction, since $2k < km = n$, by our assumption.

Therefore, we can assume that $m = 2$ and so n is even, $M = \mathrm{Sp}_n(q) \wr \mathrm{S}_2$ and V is a direct sum of two non-degenerate subspaces V_1 and V_2. Let M_0 be the pointwise stabilizer of $\{V_1, V_2\}$, so $M_0 = \mathrm{Sp}_n(q) \times \mathrm{Sp}_n(q)$. Let $\mathfrak{A}_0 = \mathfrak{A} \cap M_0$ and note that $|\mathfrak{A} : \mathfrak{A}_0| = \gcd(2, q-1)$. Also, let $L := \mathrm{Sp}_n(q) \times 1$ and $R := 1 \times \mathrm{Sp}_n(q)$, so $M_0 = L \times R$. Then, by the Second Isomorphism Theorem, we have

$$\mathfrak{A}_0/(\mathfrak{A}_0 \cap R) \cong R\mathfrak{A}_0/R \leqslant LR/R \cong L.$$

If $\mathfrak{A}_0 \cap R \neq 1$, then there is a non trivial element of $\mathfrak{A}$ that fixes every vector in V_1, which contradicts Lemma 3.1.3. So $\mathfrak{A}_0 \cap R = 1$ and $\mathfrak{A}_0$ is isomorphic to a subgroup of $\mathrm{Sp}_n(q)$. Therefore we can use the bounds on the element order of $\mathrm{Sp}_n(q)$ given in Theorem 2.2.6 to get

$$(q^n - 1) / \gcd(2, q-1) \leqslant \gcd(2, q-1)\, q^{(n+2)/2} / (q-1)\,.$$

This only gives the solutions $n = 2$ and $q = 2$, 3 or 5.

If $q = 5$, then the maximum element order in $\mathrm{Sp}_2(5)$ is 10. But$(5^2 - 1)/2 = 12$, a contradiction.

If $q = 3$, then $M = \mathrm{SL}_2(3) \wr \mathrm{S}_2$ and this contains an element order 8 from MAGMA [5]. Since there is a single conjugacy class of cyclic subgroups of order 8 in $\mathrm{Sp}_4(3)$, the Singer cycle of $\mathrm{GL}_2(3)$ lies in a conjugate of $\mathrm{SL}_2(3) \wr \mathrm{S}_2$.

Finally if $q = 2$, then as mentioned in Section 5.1, the linear Singer cycle of $\mathrm{Sp}_4(2)$ preserves a non-degenerate subspace. Therefore the linear Singer cycle lies in $M_0 = \mathrm{SL}_2(2) \times \mathrm{SL}_2(2)$ and consequently is in $M = \mathrm{Sp}_2(2) \wr \mathrm{S}_2$. This gives the result. □

This concludes the proof of Theorem 5.2.1.

Unitary Case

Now assume $X = \mathrm{GU}_{2n}(q)$. Our theorem is as follows.

Theorem 5.2.3 *Let $G \leqslant \mathrm{GU}_{2n}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Also assume that G preserves a direct sum decomposition of V, so G lies in class $\mathcal{C}_2$. Then G is contained in $\mathrm{GL}_n(q^2).2$.*

As before, by Theorem 3.2.2, the linear Singer cycle of $\mathrm{GU}_{2n}(q)$ preserves $W_1 \oplus W_2$, which means it lies in the isotropic direct sum stabilizer, which in this case is $\mathrm{GL}_n(q^2).2$. So again we can assume each V_i is non-degenerate and the direct sum stabilizer is $\mathrm{GU}_k(q) \wr \mathrm{S}_m$ where $2n = km$.

Proposition 5.2.4 *Let M be the subgroup $\mathrm{GU}_k(q) \wr \mathrm{S}_m$ of $\mathrm{GU}_{2n}(q)$, with $2n = km$. Then M does not contain a linear Singer cycle of $\mathrm{GU}_{2n}(q)$.*

Proof. As before, we assume first that $m \neq 2$. If $q^{2n} - 1$ does not have a primitive prime divisor, then $(n, q) = (3, 2)$ and $(k, m) = (1, 6)$ or $(2, 3)$. But neither $\mathrm{GU}_1(2) \wr \mathrm{S}_6$ nor $\mathrm{GU}_2(2) \wr \mathrm{S}_3$ contain elements of order 7, so cannot contain a element of order 63.

Therefore $q^{2n} - 1$ has a primitive prime divisor, r. Since

$$r \geqslant 2n + 1 = km + 1 > m,$$

we see that r must divide $|\mathrm{GU}_k(q)|$, and so divides $\prod_{i=1}^{k} \left(q^i - (-1)^i\right)$. This means that $2k \geqslant 2n = km$, a contradiction since $m \neq 2$.

So assume that $m = 2$ and $M = \mathrm{GU}_n(q) \wr \mathrm{S}_2$. Let $M_0 = \mathrm{GU}_n(q) \times \mathrm{GU}_n(q)$ and let $\mathfrak{A}_0 = \mathfrak{A} \cap M_0$. A similar argument as in Proposition 5.2.2 shows that $\mathfrak{A}_0$ is isomorphic to a subgroup of $\mathrm{GU}_n(q)$. By examining the element orders in Theorem 2.2.6, we see

$$\left(q^{2n} - 1\right) / \gcd(2, q-1) \leqslant (q+1)\left(q^{n-1} + q^2\right),$$

which gives $n = 2$ and $q = 3$ or 2. Here the maximum element orders in $\mathrm{GU}_2(2)$ and $\mathrm{GU}_2(3)$ are 6 and 12, respectively, and so using these numbers in our bounds gives a contradiction. □

This concludes the proof of Theorem 5.2.3.

Orthogonal Case

Finally, let $X = \mathrm{GO}_{2n}^{+}(q)$. Then our theorem is the following.

Theorem 5.2.5 *Let $G \leqslant \mathrm{GO}_{2n}^{+}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$. Also assume that G preserves a direct sum decomposition of V, so G lies in class $\mathcal{C}_2$. Then G is contained in $\mathrm{GL}_n(q).2$.*

We again note that by Theorem 3.2.2, the linear Singer cycle preserves the direct sum $W_1 \oplus W_2$ and so lies in the isotropic direct sum stabilizer $\mathrm{GL}_n(q).2$. Consequentially, we may assume that each V_i is non-degenerate. The stabilizer of the direct sum then is either $\mathrm{GO}_{2k}^{\varepsilon}(q) \wr \mathrm{S}_m$ where $\varepsilon = \pm$, $n = km$ and m is even when $\varepsilon = -$, or $\mathrm{GO}_k(q) \wr \mathrm{S}_m$ where $km = 2n$, kq is odd and either n is even or $q \equiv 1 \bmod 4$.

Proposition 5.2.6 *Let M be the subgroup $\mathrm{GO}_{2k}^{\varepsilon}(q) \wr \mathrm{S}_m$ of $\mathrm{GO}_{2n}^{+}(q)$, where $\varepsilon = \pm$, $n = km$ and m is even when $\varepsilon = -$. Then M does not contain a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$.*

Proof. First we assume that $m \neq 2$ when $\varepsilon = -$. If $q^n - 1$ does not have a primitive prime divisor then $(n, q) = (6, 2)$ and M is one of $\mathrm{GO}_2^{\varepsilon}(2) \wr \mathrm{S}_6$, $\mathrm{GO}_4^{\varepsilon}(2) \wr \mathrm{S}_3$ or $\mathrm{GO}_6^{+}(2) \wr \mathrm{S}_2$. But none of these groups contain an element of order 63.

So $q^n - 1$ has a primitive prime divisor, r. We have

$$r \geqslant n + 1 = km + 1 > m,$$

so r divides $|\mathrm{GO}_{2k}^{\varepsilon}(q)|$. Since $2k - 2 < km = n$ and r is a primitive prime divisor, we see that r divides $q^k \pm 1$, a contradiction.

Therefore, we may assume that $m = 2$, so $n \geqslant 4$ and $M = \mathrm{GO}_n^{-}(q) \wr \mathrm{S}_2$. By a similar argument as in the symplectic case, by Theorem 2.2.6 we see

$$(q^n - 1) / \gcd(2, q-1) \leqslant \gcd(2, q-1)\, q^{(n+2)/2} / (q-1),$$

which has no solutions for $n \geqslant 4$. □

Proposition 5.2.7 *Let M be the subgroup $\mathrm{GO}_k(q) \wr \mathrm{S}_m$ of $\mathrm{GO}_{2n}^{+}(q)$, where $km = 2n$, kq is odd and either n is even or $q \equiv 1 \bmod 4$. Then M does not contain a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$.*

Proof. By our assumption, $q^n - 1$ has a primitive prime divisor, r. Note that r cannot divide $|\mathrm{GO}_k(q)|$, since

$$k - 1 \leqslant (km - 2)/2 < n.$$

So r divides $|\mathrm{S}_m|$ and in particular $r \leqslant m$. On the other hand,

$$r \geqslant n + 1 = (km + 2)/2,$$

So $(km + 2)/2 \leqslant m$, which gives $(k - 2)m \leqslant -2$. In particular $k - 2 < 0$, so $k = 1$.

Thus $M = \mathrm{GO}_1(q) \wr \mathrm{S}_{2n}$. Using the bound for the maximum element order in symmetric groups given in [28, Proposition 3.22], we get

$$q^n - 1 \leqslant 2\mathrm{e}^{2n/\mathrm{e}},$$

which has no solutions for $n \geqslant 3$ and q a power of a prime. □

This concludes the proof of Theorem 5.2.5 and the imprimitive case.

5.3 Stabilizers of extension fields

Assume G acts primitively on V and suppose that G does not act absolutely irreducibly on V. Then G lies in class $\mathcal{C}_3$ and G lies inside an extension field-type subgroup of X. For all but two sets of groups in class $\mathcal{C}_3$, we use embeddings of extension field type groups of $\mathrm{GL}_n(q^u)$, appearing in Theorem 2.1.4 to prove the result. For the remaining two cases, we use primitive prime divisors of $q^{un} - 1$ to rule these out.

Symplectic Case

First let $X = \mathrm{Sp}_{2n}(q)$. Then there are two sets of subgroups in class $\mathcal{C}_3$. These are $\mathrm{Sp}_{2n/s}(q^s).s$, for some prime s dividing n and $\mathrm{GU}_n(q).2$ for q odd. Our Theorem in this section is the following:

Theorem 5.3.1 *Let $G \leqslant \mathrm{Sp}_{2n}(q)$ and suppose that G contains a linear Singer cycle of* $\mathrm{Sp}_{2n}(q)$. *Assume that G lies inside class $\mathcal{C}_3$ so is contained in an extension field-type subgroup of* $\mathrm{Sp}_{2n}(q)$. *Then either G is contained in* $\mathrm{Sp}_{2n/s}(q^s).s$ *for some prime s dividing n, or n is even, q is odd and G is contained in* $\mathrm{GU}_n(q).2$.

We first show that the subgroups, $\mathrm{Sp}_{2n/s}(q^s).s$ contain a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$.

Proposition 5.3.2 *If s is a prime dividing n, then the subgroups* $\mathrm{Sp}_{2n/s}(q^s).s$ *of* $\mathrm{Sp}_{2n}(q)$ *contain the linear Singer cycle of* $\mathrm{Sp}_{2n}(q)$.

Proof. There are embeddings of $\mathrm{GL}_{n/s}(q^s)$ into $\mathrm{Sp}_{2n/s}(q^s)$ as well as $\mathrm{GL}_n(q)$ illustrated in Figure 5.1. By Theorem 2.1.4, the Singer cycle of $\mathrm{GL}_n(q)$ lies in a conjugate of $\mathrm{GL}_{n/s}(q^s)$

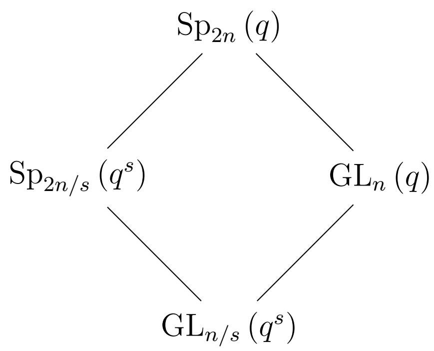

Figure 5.1: Embedding $\mathrm{GL}_{n/s}(q^s)$ into $\mathrm{Sp}_{2n/s}(q^s)$ and $\mathrm{GL}_n(q)$

and so lies in a conjugate of $\mathrm{Sp}_{2n/s}(q^s)$. Hence it lies in a conjugate of $\mathrm{Sp}_{2n/s}(q^s).s$. □

For $\mathrm{GU}_n(q).2$, we distinguish between the cases when n is odd and when n is even.

Proposition 5.3.3 *If n is even and q is odd, then the subgroups* $\mathrm{GU}_n(q).2$ *of* $\mathrm{Sp}_{2n}(q)$ *contain the linear Singer cycle of* $\mathrm{Sp}_{2n}(q)$.

Proof. We have embeddings of $\mathrm{GL}_{n/2}(q^2)$ into $\mathrm{GU}_n(q)$ and $\mathrm{GL}_n(q)$. The partial subgroup lattice of these groups in $\mathrm{Sp}_{2n}(q)$ is shown in Figure 5.2.

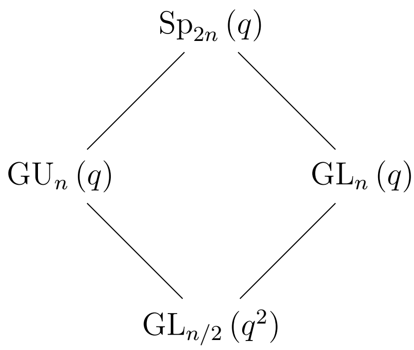

Figure 5.2: Embedding $\mathrm{GL}_{n/2}(q^2)$ into $\mathrm{GU}_n(q)$ and $\mathrm{GL}_n(q)$.

As before, the Singer cycle of $\mathrm{GL}_n(q)$ lies in a conjugate of $\mathrm{GL}_{n/2}(q^2)$ by Theorem 2.1.4 and hence lies in a conjugate of $\mathrm{GU}_n(q)$. Therefore it lies in a conjugate of $\mathrm{GU}_n(q).2$. □

If n is odd, then $\mathrm{GU}_n(q).2$ does not contain a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$, or in fact any element of order $q^n - 1$. This follows directly from the following proposition.

Proposition 5.3.4 *Let nq be odd. Then the order of $\mathrm{GU}_n(q).2$ is not divisible by a primitive prime divisor of $q^n - 1$.*

Proof. Note that since n is odd, a primitive prime divisor of $q^n - 1$ exists. Let r be such a prime that divides the order of $\mathrm{GU}_n(q).2$. We know r cannot be 2, so r divides the order of $\mathrm{GU}_n(q)$. We can write

$$|\mathrm{GU}_n(q)| = q^{n(n-1)/2} \prod_{k=1}^{(n+1)/2} \left(q^{2k-1}+1\right) \prod_{k=1}^{(n-1)/2} \left(q^{2k}-1\right).$$

Now r cannot divide q, since q and $q^n - 1$ are coprime, nor can it divide $q^{2k} - 1$ for $1 \leqslant k \leqslant (n-1)/2$ since $2k < n$. Also r does not divide $q^n + 1$, since the greatest common divisor of $q^n - 1$ and $q^n + 1$ divides 2. Therefore r must divide one of the $q^{2k-1} + 1$ for $1 \leqslant k < (n+1)/2$, so r divides

$$\left(q^{2k-1}+1\right)\left(q^{2k-1}-1\right) = q^{2(2k-1)} - 1.$$

Consider $\gcd(q^m - 1, q^n - 1)$ where $m := 2(2k-1)$. By [19, Hilfssatz 2a], this is equal to $q^{\gcd(m,n)} - 1$ and note that $\gcd(m,n) \leqslant n$. If $\gcd(m,n) = n$ then n divides m. But then, since $m/2 < n$, this forces $m = n$, contrary to n being odd.

So $\gcd(m,n) < n$. But r divides $\gcd(q^m - 1, q^n - 1)$ which contradicts the assumption that r is a primitive prime divisor. Thus the order of $\mathrm{GU}_n(q).2$ cannot be divisible by a primitive prime divisor of $q^n - 1$. □

Propositions 5.3.2, 5.3.3 and 5.3.4 together prove Theorem 5.3.1.

Unitary Case

Now assume that $X = \mathrm{GU}_{2n}(q)$. In this case, there is only one set of subgroups in class $\mathcal{C}_3$. These have the structure $\mathrm{GU}_{2n/s}(q^s).s$, where s is an odd prime. Our Theorem in this section is the following.

Theorem 5.3.5 *Let $G \leqslant \mathrm{GU}_{2n}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Assume that G lies inside class $\mathcal{C}_3$ so is contained in an extension field-type subgroup of $\mathrm{GU}_{2n}(q)$. Then G is contained in $\mathrm{GU}_{2n/s}(q).s$, where s is an odd prime.*

Proof. Since there is only one set of subgroups in class $\mathcal{C}_3$ in this case, we only need to show that $\mathrm{GU}_{2n/s}(q^s).s$ contains the linear Singer cycle of $\mathrm{GU}_{2n}(q)$. We argue as in Proposition 5.3.2.

We have embeddings of $\mathrm{GL}_{n/s}(q^{2s})$ into $\mathrm{GU}_{2n/s}(q^s)$ and $\mathrm{GL}_n(q^2)$. The partial subgroup lattice is shown in Figure 5.3. By Theorem 2.1.4, the Singer cycle of $\mathrm{GL}_n(q^2)$ lies in a conjugate of $\mathrm{GL}_{n/s}(q^{2s})$ and hence lies in a conjugate of $\mathrm{GU}_{2n/s}(q^s)$. Therefore the Singer cycle of $\mathrm{GL}_n(q^2)$ lies in a conjugate $\mathrm{GU}_{2n/s}(q^s).s$. □

Orthogonal Case

Now let $X = \mathrm{GO}^+_{2n}(q)$. There are three sets of subgroups in class $\mathcal{C}_3$. These are $\mathrm{GO}^+_{2n/s}(q^s).s$ with s a prime dividing n, $\mathrm{GU}_n(q).2$ with n even, and $\mathrm{GO}_n(q^2).2$ with

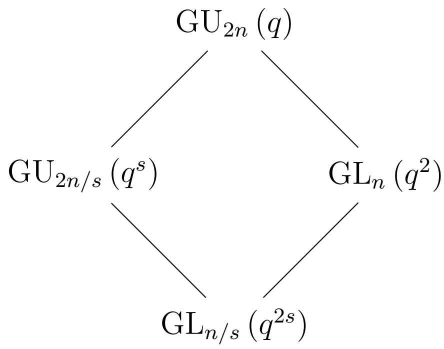

Figure 5.3: Embeddings of $\mathrm{GL}_{n/s}(q^{2s})$ into $\mathrm{GU}_{2n/s}(q^s)$ and $\mathrm{GL}_n(q^2)$.

nq odd. Our main theorem in this section is the following.

Theorem 5.3.6 *Let $G \leqslant \mathrm{GO}^+_{2n}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GO}^+_{2n}(q)$. Assume that G lies inside class $\mathcal{C}_3$ so is contained in an extension field-type subgroup of $\mathrm{GO}^+_{2n}(q)$. Then either G is contained in $\mathrm{GO}^+_{2n/s}(q^s).s$ for some prime s dividing n, or n is even and G is contained in $\mathrm{GU}_n(q).2$.*

The $\mathrm{GO}^+_{2n/s}(q^s).s$ and the $\mathrm{GU}_n(q).2$ cases are dealt with the same methods as before. In fact the $\mathrm{GU}_n(q).2$ case is very similar to Proposition 5.3.3.

Proposition 5.3.7 *If s is prime, then the subgroups $\mathrm{GO}^+_{2n/s}(q^s).s$ of $\mathrm{GO}^+_{2n}(q)$ contain the linear Singer cycle of $\mathrm{GO}^+_{2n}(q)$.*

Proof. There are embeddings of $\mathrm{GL}_{n/s}(q^s)$ into $\mathrm{GO}^+_{2n/s}(q^s)$ and $\mathrm{GL}_{n/s}(q^s)$ illustrated in Figure 5.4. The Singer cycle of $\mathrm{GL}_n(q)$ lies in a conjugate of $\mathrm{GL}_{n/s}(q^s)$ and hence lies in a conjugate of $\mathrm{GO}^+_{2n/s}(q^s)$. Therefore the Singer cycle of $\mathrm{GL}_n(q)$ lies in a conjugate of $\mathrm{GO}^+_{2n/s}(q^s).s$. □

Proposition 5.3.8 *If n is even, then the subgroups $\mathrm{GU}_n(q).2$ of $\mathrm{GO}^+_{2n}(q)$ contain the linear Singer cycle of $\mathrm{GO}^+_{2n}(q)$.*

Proof. See Proposition 5.3.3. □

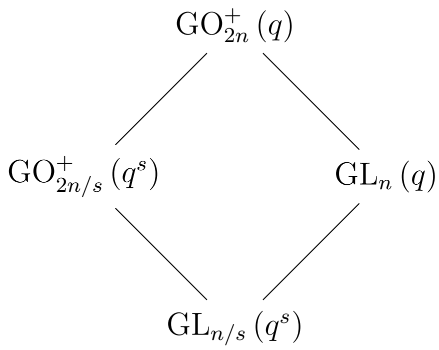

Figure 5.4: Embeddings of $\mathrm{GL}_{n/s}(q^s)$ into $\mathrm{GO}_{2n/s}^{+}(q^s)$ and $\mathrm{GL}_{n/s}(q^s)$

As in Proposition 5.3.4, $\mathrm{GO}_n(q^2).2$ does not contain a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$, or any element of order $q^n - 1$. This is a result of the following Proposition.

Proposition 5.3.9 *Let nq be odd. Then the order of $\mathrm{GO}_n(q^2).2$ is not divisible by a primitive prime divisor of $q^n - 1$.*

Proof. By our assumptions, $q^n - 1$ has a primitive prime divisor, r. Suppose that r divides the order of $\mathrm{GO}_n(q^2).2$. Then r divides

$$\left|\mathrm{GO}_n\left(q^2\right).2\right| = 4q^{(n-1)^2/2} \prod_{i=1}^{(n-1)/2} \left(q^{4i} - 1\right).$$

Obviously r does not divide 4 or $q^{(n-1)^2/2}$ and so r must divide $\prod_{i=1}^{(n-1)/2}(q^{4i} - 1)$. But, since n is odd, $q^n - 1$ is not one of the terms in the product and

$$4((n-1)/2) = 2n - 2 < 2n.$$

This gives a contradiction. □

Propositions 5.3.7, 5.3.8 and 5.3.9 together prove Theorem 5.3.6. This concludes the case of the extension field-type subgroups.

5.4 Stabilizers of tensor product decompositions

We now assume that G acts absolutely irreducibly on V. Suppose that G lies in class $\mathcal{C}_4$. That is G preserves a tensor product decomposition of the form $V = V_1 \otimes V_2$ with $\dim(V_1) \neq \dim(V_2)$. We will use primitive prime divisors of $q^{un} - 1$ to obtain conditions on $\dim(V_1)$ and $\dim(V_2)$. We then apply the element order bounds from Theorem 2.2.6 and use MAGMA to consider any remaining cases. We will show that these groups do not contain a linear Singer cycle except for just one case in $\mathrm{GO}_8^+(2)$.

Symplectic Case

We first assume that $X = \mathrm{Sp}_{2n}(q)$. In this case q is odd and G is contained in the group

$$(\mathrm{Sp}_{2k}(q) \circ \mathrm{GO}_m^{\varepsilon}(q)) \,.\, \gcd(m, 2),$$

with $n = km$, $\varepsilon \in \{-, \circ, +\}$ and $m \geqslant 3$. Our theorem in this section shows that this case does not arise.

Theorem 5.4.1 *Let $G \leqslant \mathrm{Sp}_{2n}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. Then $G \notin \mathcal{C}_4$.*

Proof. Suppose otherwise. Then as mentioned above, q is odd and G is contained in

$$M := (\mathrm{Sp}_{2k}(q) \circ \mathrm{GO}_m^{\varepsilon}(q)) \,.\, \gcd(m, 2),$$

where $n = km$, $\varepsilon \in \{-, \circ, +\}$ and $m \geqslant 3$. If M contained a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$, then the order of the group,

$$\widetilde{M} := \mathrm{Sp}_{2k}(q) \times \mathrm{GO}_m^{\varepsilon}(q)$$

must be divisible by $q^n - 1$. Now $m \geqslant 3$ and $n = km$, which implies $n \geqslant 3$ and so since q is odd, $q^n - 1$ has a primitive prime divisor, r, which must divide the order of $\widetilde{M}$. We know that r cannot divide any power of q and since $m \geqslant 3$, we have $2k < n$, which means that r does not divide $\prod_{i=1}^{k} (q^{2i} - 1)$. Therefore r cannot divide the order of $\mathrm{Sp}_{2k}(q)$ and so divides the order of $\mathrm{GO}_m^{\varepsilon}(q)$.

If $\varepsilon = \circ$, then r must divide $\prod_{i=1}^{(m-1)/2} (q^{2i} - 1)$. But $m - 1 < km = n$ which is a contradiction. So $\varepsilon \neq \circ$ and since we also have $m-2 < n$, r does not divide $\prod_{i=1}^{(m-2)/2} (q^{2i} - 1)$ and so r must divide $q^{m/2} - \varepsilon 1$. If $\varepsilon = +$, then r divides $q^{m/2} - 1$ and since $m/2 < n$, we get a contradiction. So $\varepsilon = -$ and r divides $q^{m/2} + 1$ and so divides $q^m - 1$, which is also a contradiction unless $n = m$.

Suppose now that $m = n$ and $\varepsilon = -$. Then n is even and M is of the form

$$\left(\mathrm{Sp}_2(q) \circ \mathrm{GO}_n^-(q)\right).2 \cong \left(\mathrm{SL}_2(q) \circ \mathrm{GO}_n^-(q)\right).2.$$

Now the image of M in $\mathrm{PSp}_{2n}(q)$ is $\overline{M} := \left(\mathrm{PSL}_2(q) \times \mathrm{PGO}_n^-(q)\right).2$ and since M contains a linear Singer cycle, $\overline{M}$ has to contain an element of order $(q^n - 1)/2$. We will now use the element order bounds in Theorem 2.2.6 to obtain a contradiction.

If $n \geqslant 8$, then an upper bound for the element order of $\overline{M}$ is

$$(q+1) \cdot q^{(n+2)/2} \cdot 2/(q-1) = 2q^{(n+2)/2}(q+1)/(q-1),$$

by Theorem 2.2.6. So since $\overline{M}$ contains an element of order $(q^n - 1)/2$, we must have

$$(q^n - 1)/2 \leqslant 2q^{(n+2)/2}(q+1)/(q-1).$$

But this inequality has no integer solutions for $n \geqslant 8$ and q a power of an odd prime.

If $n = 6$, then $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$, so this time the maximum element order in $\overline{M}$ is at most

$$(q+1)\cdot\left(q^3+1\right)\cdot 2.$$

As before, if $\overline{M}$ contains an element of order $(q^n-1)/2$, we have

$$\left(q^6-1\right)/2 \leqslant (q+1)\cdot 2q^4\cdot 2 = 4q^4(q+1).$$

Again this inequality has no solutions for q a power of an odd prime.

Therefore we have $n=4$. Note that $\mathrm{P}\Omega_4^-(q)\cong \mathrm{PSL}_2(q^2)$, so this time an upper bound on the element order of $\overline{M}$ is $2(q+1)(q^2+1)$. Assuming that $\overline{M}$ has an element of order $(q^n-1)/2$, we get

$$\left(q^4-1\right)/2 \leqslant 2(q+1)\left(q^2+1\right),$$

which gives $q=3$ or 5. If $q=5$ then since the maximum element orders in $\mathrm{PSL}_2(5)$ and $\mathrm{PGO}_4^-(5)$ are 5 and 13, respectively, an upper bound on the element order of $\overline{M}$ is $5\cdot 13\cdot 2=130$. But in this case

$$(q^n-1)/2 = 312 > 130.$$

Therefore $q=3$. Here, the maximum element orders in $\mathrm{PSL}_2(3)$ and $\mathrm{PGO}_4^-(3)$ are 3 and 6 and so the maximum element order of $\overline{M}$ is at most $3\cdot 6\cdot 2=36$. But

$$(q^n-1)/2 = 40 > 36.$$

This contradiction concludes the proof of the theorem. □

Unitary Case

Now suppose that $X=\mathrm{GU}_{2n}(q)$. Then G is contained in the group $\mathrm{GU}_k(q)\circ\mathrm{GU}_m(q)$ where $2n=km$. Our main theorem in this section is the following.

Theorem 5.4.2 *Let $n \geqslant 2$ and let $G \leqslant \mathrm{GU}_{2n}(q)$. Suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Then $G \notin \mathcal{C}_4$.*

Proof. If G lies in $\mathcal{C}_4$ then as mentioned above, G is contained in the group

$$M := \mathrm{GU}_k(q) \circ \mathrm{GU}_m(q)$$

with $2n = km$ and $k \neq m$. Without loss of generality, we can assume that $k > m$. Suppose first that $m > 2$. Then $q^{2n} - 1$ has a primitive prime divisor, r. If M contains a linear Singer cycle, then r divides the order of M and so divides $|\mathrm{GU}_k(q)|$ or $|\mathrm{GU}_m(q)|$. If r divides the order of $\mathrm{GU}_m(q)$, then r divides an expression of the form $q^i - (-1)^i$, for $1 \leqslant i \leqslant m$. But $2k < km = 2n$, so this cannot happen.

So we may assume that r divides the order of $\mathrm{GU}_k(q)$. Then, r must divide an expression of the form $q^i - (-1)^i$, for $1 \leqslant i \leqslant k$. Since $m \neq 2$, we have $2k < km = 2n$ which gives a contradiction.

Therefore we can assume that $m = 2$, and $k = n$. Then M becomes

$$\mathrm{GU}_n(q) \circ \mathrm{GU}_2(q).$$

If n is even, then a primitive prime divisor of $q^{2n} - 1$ exists and must divide the order of M, given that M contains a linear Singer cycle. We can assume that r divides the order of $\mathrm{GU}_n(q)$. This means r either divides $q^k - 1$ or an expression of the form $q^i - (-1)^i$, for $1 \leqslant i \leqslant k - 1$. But

$$k < 2k - 2 < 2k = 2n,$$

so this cannot happen.

Thus n is odd. Note that the image of M in $\mathrm{PGU}_{2n}(q)$ is

$$\overline{M} := \mathrm{PGU}_n(q) \times \mathrm{PGU}_2(q) \cong \mathrm{PGU}_n(q) \times \mathrm{PGL}_2(q).$$

If M contained a linear Singer cycle, then $\overline{M}$ contains an element of order $(q^{2n}-1)/(q+1)$. By Theorem 2.2.6, the maximum possible element order in $\overline{M}$ is $q(q^{n-2}+1)\cdot(q+1)$. Therefore if $\overline{M}$ contains an element of order $(q^{2n}-1)/(q+1)$, we must have

$$\left(q^{2n}-1\right)/(q+1) \leqslant q\left(q^{n-2}+1\right)(q+1).$$

But this inequality has no integer solutions with $n \geqslant 3$ odd and q a power of a prime. This concludes the proof of the theorem. □

Orthogonal Case

Suppose that $X = \mathrm{GO}_{2n}^{+}(q)$. Then there are three sets of groups in class $\mathcal{C}_4$. These are

$$(\mathrm{Sp}_{2k}(q) \circ \mathrm{Sp}_{2m}(q)).\gcd(2, q-1),$$

where $n = 2km$;

$$\mathrm{GO}_{2k}^{+}(q) \times \mathrm{SO}_m(q),$$

with $n = km$ and mq odd and

$$(\mathrm{GO}_{2k}^{\varepsilon_1}(q) \circ \mathrm{GO}_{2m}^{\varepsilon_2}(q)).2,$$

where $m \geqslant 2$, $n = 2km$, $\varepsilon_i = \pm$ and q is odd. Our main theorem is the following.

Theorem 5.4.3 *Let $n \geqslant 3$ and let $G \leqslant \mathrm{GO}_{2n}^{+}(q)$. Suppose that G contains a linear*

Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$ *and that* $G \in \mathcal{C}_4$*. Then* $(n,q) = (4,2)$ *and* G *is contained in*

$$\mathrm{Sp}_4(2) \circ \mathrm{Sp}_2(2) \cong \mathrm{S}_6 \times \mathrm{S}_3.$$

We begin with the first set of groups in $\mathcal{C}_4$.

Proposition 5.4.4 *Let* $n \geqslant 3$ *and*

$$M = (\mathrm{Sp}_{2k}(q) \circ \mathrm{Sp}_{2m}(q)) \,.\, \gcd(2, q-1),$$

where $n = 2km$*. Suppose further that* M *contains a linear Singer cycle of* $\mathrm{GO}_{2n}^{+}(q)$*. Then* $(n,q) = (4,2)$*.*

Proof. Without loss of generality, we can assume that $k > m$. Suppose first that $m > 1$. Then $q^n - 1$ has a primitive prime divisor, r. If M contains a linear Singer cycle, then r divides the order of M and so divides $|\mathrm{Sp}_{2k}(q)|$ or $|\mathrm{Sp}_{2m}(q)|$. If r divides the order of $\mathrm{Sp}_{2m}(q)$, then r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant m$. But $2m < 2km = n$, so this cannot happen.

Hence we may assume that r divides the order of $\mathrm{Sp}_{2k}(q)$. Then r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant k$. But then $2k < 2km = n$, which gives a contradiction.

So we can assume $m = 1$. So $n = 2k$ and

$$M = (\mathrm{Sp}_n(q) \circ \mathrm{Sp}_2(q)) \,.\, \gcd(2, q-1) \cong (\mathrm{Sp}_n(q) \circ \mathrm{SL}_2(q)) \,.\, \gcd(2, q-1).$$

Observe that the image of M in $\mathrm{PGO}_{2n}^{+}(q)$ is

$$\overline{M} := (\mathrm{PSp}_n(q) \times \mathrm{PSL}_2(q)) \,.\, \gcd(2, q-1).$$

If M contains a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$, then $\overline{M}$ contains an element of order

$(q^n - 1) / \gcd(2, q-1)$. By Theorem 2.2.6, an upper bound for the element order of $\overline{M}$ is

$$\left(q^{(n+2)/2} / (q-1)\right) \cdot (q+1) \cdot \gcd(2, q-1).$$

We therefore have to have

$$(q^n - 1) / \gcd(2, q-1) \leqslant \gcd(2, q-1)\, q^{(n+2)/2} (q+1) / (q-1).$$

The only integer solutions to this inequality with $n \geqslant 4$ and q a power of a prime, are $n = 4$ and $q = 2$, 3 or 5.

If $q = 5$, then the largest element orders in $\mathrm{PSp}_4(5)$ and $\mathrm{PSL}_2(5)$ are 30 and 5, respectively, so the largest possible element order in $\overline{M}$ is 300. But $(q^4 - 1) / \gcd(2, q-1) = 312$, a contradiction. If $q = 3$, then we can observe that 5 divides $(q^4 - 1) / \gcd(2, q-1)$ but doesn't divide the order of $\overline{M}$, so this case is also ruled out.

This leaves us the case when $q = 2$. Here $q^n - 1 = 15$ and

$$M = \mathrm{Sp}_4(2) \times \mathrm{Sp}_2(2) \cong \mathrm{S}_6 \times \mathrm{S}_3.$$

In $\mathrm{GO}_8^+(2)$, there are two conjugacy classes of subgroups of order 15. One class contains subgroups whose centralizer has order 30, the other contains self centralizing subgroups. Hence by Proposition 3.3.2, the linear Singer cycle is contained in a conjugate of a subgroup of $\mathrm{GO}_8^+(q)$ that contains a self-centralizing subgroup of order 15. From the MAGMA code in Appendix A.1, M contains a self centralizing subgroup of order 15. Therefore the linear Singer cycle is contained in a conjugate of M. □

Now all that is left to do is to rule out the other cases. This will follow from the following two results.

Proposition 5.4.5 *Let $n = km$ and mq be odd. Then the order of $M := \mathrm{GO}_{2k}^{+}(q) \times \mathrm{SO}_m(q)$ is not divisible by a primitive prime divisor of $q^n - 1$.*

Proof. Since mq is odd, $q^n - 1$ does indeed have a primitive prime divisor. Let r be such a prime divisor and suppose that r divides the order of M. If r divides $|\mathrm{SO}_m(q)|$, then r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant (m-1)/2$. This cannot happen because

$$m - 1 \leqslant km - 1 < n.$$

Therefore r divides $\left|\mathrm{GO}_{2k}^{+}(q)\right|$ and so divides either $q^k - 1$ or an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant k - 1$. But $k < km = n$ and

$$2k - 2 < km - 2 < n.$$

The result follows. □

Proposition 5.4.6 *Let $n = 2km$ and q be odd. Also let $m \geqslant 2$ and $\varepsilon_i \in \{-, +\}$. Then the order of $M := (\mathrm{GO}_{2k}^{\varepsilon_1}(q) \circ \mathrm{GO}_{2m}^{\varepsilon_2}(q)).2$ is not divisible by a primitive prime divisor of $q^n - 1$.*

Proof. Note that since q is odd, a primitive prime divisor of $q^n - 1$ exists, so let r be such a prime divisor. Assuming r divides the order of M, we observe r divides either $|\mathrm{GO}_{2k}^{\varepsilon_1}(q)|$ or $|\mathrm{GO}_{2m}^{\varepsilon_2}(q)|$. By relabeling if necessary, we may assume that r divides the order of $\mathrm{GO}_{2k}^{\varepsilon_1}(q)$. Note r cannot divide $q^k - \varepsilon_1 1$ as

$$k < 2k < 2km = n,$$

therefore r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant k - 1$. But

$$2k - 2 < 2km - 2 < n,$$

which cannot happen. □

Propositions 5.4.4, 5.4.5 and 5.4.6 together give the proof of Theorem 5.4.3.

5.5 Stabilizers of subfields

Assume that G lies in class $\mathcal{C}_5$, so G is contained in the stabilizer of a subfield of $\mathrm{GF}(q^u)$ of prime index. As before, we use primitive prime divisors of $q^{un}-1$ and the element order bounds in Theorem 2.2.6 to deal with this case. We will show that these groups do not contain a linear Singer cycle of X except in just one case when $X = \mathrm{GU}_4(2)$.

Symplectic Case

Suppose first that $X = \mathrm{Sp}_{2n}(q)$. Then $q = q_0^m$, where m is prime and G is contained in the group

$$M := \begin{cases} \mathrm{Sp}_{2n}(q_0).2, & \text{if } m = 2 \text{ and } q \text{ is odd}, \\ \mathrm{Sp}_{2n}(q_0), & \text{otherwise.} \end{cases}$$

Our Theorem in this section is the following.

Theorem 5.5.1 *Let $n \geqslant 2$ and $G \leqslant \mathrm{Sp}_{2n}(q)$. If G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$, then $G \notin \mathcal{C}_5$.*

Proof. Suppose $G \in \mathcal{C}_5$, so $q = q_0^m$ for some prime m and let M be as above. We will show that M cannot contain any element of order $q^n - 1$, to obtain a contradiction.

Suppose first that $m \neq 2$ so $mn \geqslant 6$. If $q_0 = 2$ and $mn = 6$, then $n = 2$ and $q^n - 1 = 63$. On the other hand, $M = \mathrm{Sp}_4(2)$, which obviously contains no element of order 63.

Therefore, $q_0^{mn} - 1$ has a primitive prime divisor, r. If M contains an element of order $q^n - 1$, then r divides the order of M. Hence r divides an expression of the form $q_0^{2i} - 1$, for $1 \leqslant i \leqslant n$. Since $2n < mn$, this is a contradiction.

So assume $m = 2$ and $M = \mathrm{Sp}_{2n}(q_0) \,.\, \gcd(2, q-1)$. By 2.2.6, an upper bound for the element order in M is

$$\gcd(2, q-1) \cdot \left(q_0^{n+1} / (q_0 - 1)\right) \cdot \gcd(2, q-1) = \gcd(2, q-1)^2 \, q_0^{n+1} / (q_0 - 1) \,.$$

If M contained an element of order $q^n - 1$, we get

$$q_0^{2n} - 1 \leqslant \gcd(2, q-1)^2 \, q_0^{n+1} / (q_0 - 1) \,,$$

which has no integer solutions for $n \geqslant 2$ and q_0 a power of a prime.

This contradiction shows M cannot contain an element of order $q^n - 1$ and proves the theorem. □

Unitary Case

Now suppose that $X = \mathrm{GU}_{2n}(q)$. There are three sets of groups in class $\mathcal{C}_5$. These are $C_{q+1}.\mathrm{PGU}_{2n}(q_0)$, where $q_0^m = q$ with m an odd prime, $C_{q+1} \circ \mathrm{GO}^{\pm}_{2n}(q)$, for q odd and $C_{q+1} \circ \mathrm{Sp}_{2n}(q)$. Our theorem is the following.

Theorem 5.5.2 *Let $n \geqslant 2$ and let $G \leqslant \mathrm{GU}_{2n}(q)$. Suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$ and that $G \in \mathcal{C}_5$. Then $(n, q) = (2, 2)$ and G is contained in* $\mathrm{C}_3 \circ \mathrm{Sp}_4(2) \cong 3 \times \mathrm{S}_6$.

We first rule out the $\mathrm{C}_{q+1}.\mathrm{PGU}_{2n}(q_0)$ case. This follows immediately from the following proposition.

Proposition 5.5.3 *Let $q = q_0^m$ with m an odd prime. Then the order of $C_{q+1}.\mathrm{PGU}_{2n}(q_0)$ is not divisible by a primitive prime divisor of $q_0^{mn} - 1$.*

Proof. Since $n \geqslant 2$ and m is an odd prime, $q_o^{2nm} - 1$ does indeed primitive prime divisor. Let r be such a prime divisor and suppose that r divides the order of $C_{q+1}.\mathrm{PGU}_{2n}(q_0)$. If

r divides $q+1$, then r divides $q^2-1=q_0^{2m}-1$, which cannot happen. So r divides the order of $\mathrm{PGU}_{2n}(q_0)$ and so divides an expression of the form $q_0^i-(-1)^i$, for $1\leqslant i\leqslant 2n$. But $4n<2nm$, a contradiction. □

Proposition 5.5.4 *Let q be odd and $M=C_{q+1}\circ \mathrm{GO}_{2n}^{\varepsilon}(q)$ where $\varepsilon=\pm$. Then M does not contain a linear Singer cycle of* $\mathrm{GU}_{2n}(q)$.

Proof. Assume that M contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Suppose first that $\varepsilon=+$. Since q is odd, $q^{2n}-1$ has a primitive prime divisor, r. If M contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, then r divides the order of M. We know that r cannot divide $q+1$, $q^{n(n-1)}$ or q^n-1, so it must divide an expression of the form $q^{2i}-1$, where $1\leqslant i\leqslant n-1$. But $2n-2<2n$, a contradiction.

So we may assume that $\varepsilon=-$. The quotient group,

$$\overline{M}=C_{(q+1)/2}\times \mathrm{PGO}_{2n}^{-}(q)$$

of M contains an element of order $(q^{2n}-1)/2$, by our assumption. If $n\geqslant 4$, then by Theorem 2.2.6, an upper bound on the element order of $\overline{M}$ is

$$((q+1)/2)\cdot\left(q^{n+1}/(q-1)\right)=q^{n+1}(q+1)/2(q-1).$$

Since $\overline{M}$ contains an element of order $(q^{2n}-1)/2$, we must have

$$\left(q^{2n}-1\right)/2\leqslant q^{n+1}(q+1)/2(q-1).$$

But this inequality has no integer solutions for $n\geqslant 4$ and q an odd power of a prime.

If $n=3$, then using the fact that $\mathrm{P}\Omega_6^{-}(q)\cong \mathrm{PSU}_4(q)$ and Theorem 2.2.6, an upper bound on the element order of $\overline{M}$ is

$$((q+1)/2) \cdot \left(q^3+1\right).$$

Again, using our assumptions,

$$\left(q^6-1\right)/2 \leqslant (q+1)\left(q^3+1\right)/2,$$

which again has no integer solutions for q an odd power of a prime.

So we can assume $n=2$. In this case using Theorem 2.2.6 and noting $\mathrm{P\Omega}_4^-(q) \cong \mathrm{PSL}_2(q^2)$, an upper bound on the element order of $\overline{M}$ is

$$((q+1)/2) \cdot \left(q^2+1\right).$$

Hence, using our assumptions again, we get

$$\left(q^4-1\right)/2 \leqslant (q+1)\left(q^2+1\right)/2.,$$

But again this inequality has no integer solutions for q an odd power of a prime.

Therefore we can conclude that M cannot contain a linear Singer cycle of $\mathrm{GU}_{2n}(q)$.□

Proposition 5.5.5 *Let* $M := \mathrm{C}_{q+1} \circ \mathrm{Sp}_{2n}(q)$ *and suppose that* M *contains a linear Singer cycle of* $\mathrm{GU}_{2n}(q)$. *Then* $(n,q)=(2,2)$.

Proof. Suppose that M contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. By our assumption, the quotient group,

$$\overline{M} := \mathrm{C}_{(q+1)/\gcd(2,q-1)} \times \mathrm{PSp}_{2n}(q)$$

of M contains an element of order $(q^{2n}-1)/\gcd(2,q-1)$. Using Theorem 2.2.6, an upper bound for the element order in $\overline{M}$ is

$$((q+1)\,/\,\gcd(2,q-1))\cdot\left(q^{n+1}/\,(q-1)\right).$$

Hence, since $\overline{M}$ contains an element of order $(q^{2n}-1)\,/\,\gcd(2,q-1)$, we must have

$$\left(q^{2n}-1\right)/\gcd(2,q-1)\leqslant(q+1)\,q^{n+1}/\gcd(2,q-1)\,(q-1)\,.$$

Since $n\geqslant 2$ and q is a power of a prime, the only integer solution to this inequality is $(n,q)=(2,2)$.

In this case

$$M=\mathrm{C}_3\circ\mathrm{Sp}_4(2)\cong 3\times\mathrm{S}_6$$

and the linear Singer cycle of $\mathrm{GU}_4(2)$ has order 15. Using MAGMA [5], we can see all subgroups of order 15 in $\mathrm{GU}_4(2)$ are conjugate and M clearly contains a subgroup of order 15, therefore the linear Singer cycle is contained in a conjugate of M. □

Propositions 5.5.3, 5.5.4 and 5.5.5 form the proof of Theorem 5.5.2.

Orthogonal Case

So we can assume that $X=\mathrm{GO}^{+}_{2n}(q)$. Here $q=q_0^m$, where m is prime and G is contained in $M:=\mathrm{GO}^{\varepsilon}_{2n}(q_0)$, where $\varepsilon=\pm$ and $m=2$ when $\varepsilon=-$. Our main theorem is the following.

Theorem 5.5.6 *Let $n\geqslant 3$ and $G\leqslant\mathrm{GO}^{+}_{2n}(q)$. If G contains a linear Singer cycle of $\mathrm{GO}^{+}_{2n}(q)$, then $G\notin\mathcal{C}_5$.*

Proof. Suppose $G\in\mathcal{C}_5$, so $q=q_0^m$ for some prime m and let M be as above. We show that M does not have an element of order q^n-1, to obtain a contradiction.

Suppose otherwise and first assume $\varepsilon = +$. If $q_0 = 2$ and $kn = 6$ then $k = 2$, $n = 3$. But then $M = \mathrm{GO}_6^+(2)$ has no element of order 63.

Therefore $q_0^{kn} - 1$ has a primitive prime divisor, r, which divides the order of M by our assumption. This implies that r divides an expression of the form $q_0^{2i} - 1$, for $1 \leqslant i \leqslant n-1$. But $2(n-1) < 2n \leqslant kn$, a contradiction.

So we may assume that $\varepsilon = -$ and so $m = 2$. We again use the element order bounds in Theorem 2.2.6 to rule out these cases. If $n \geqslant 4$, then an upper bound for the element order in M is

$$\gcd(2, q_0 - 1) \cdot q_0^{n+1} / (q_0 - 1).$$

Therefore by our assumption we have

$$q_0^{2n} - 1 \leqslant \gcd(2, q_0 - 1) \cdot q_0^{n+1} / (q_0 - 1).$$

But this inequality has no integer solutions for $n \geqslant 4$ and q_0 a power of a prime.

Therefore $n = 3$. If $q_0 > 2$ then since $\mathrm{P}\Omega_6^-(q_0) \cong \mathrm{PSU}_4(q_0)$ and using Theorem 2.2.6, an upper bound on the element order of M is $\gcd(2, q_0 - 1)(q^3 + 1)$ and so by our assumption we get

$$\left(q_0^6 - 1\right) \leqslant \gcd(2, q_0 - 1)\left(q^3 + 1\right).$$

This again has no integer solutions for q_0 a power of a prime. So $q_0 = 2$ and $q^n - 1 = 63$. But $M = \mathrm{GO}_6^-(2)$ has no elements of such order.

Therefore that M cannot contain an element of order $q^n - 1$. This concludes the proof of the theorem. □

This concludes the case of the subfield stabilizers.

5.6 Normalizers of symplectic-type groups

Now assume that G lies in class $\mathcal{C}_6$. Then G normalizes a symplectic-type r-group lying in an absolutely irreducible representation, where r is a prime different to p. We use the element order bounds from Theorem 2.2.6 to show that these groups do not contain a linear Singer cycle of X except in just one case when $X = \mathrm{Sp}_4(3)$.

Symplectic Case

Assume $X = \mathrm{Sp}_{2n}(q)$. Then q is an odd prime and G lies in the group

$$M := \begin{cases} 2_-^{1+2m}.\Omega_{2m}^-(2), & \text{when } q \equiv \pm 3 \pmod 8, \\ 2_-^{1+2m}.\mathrm{GO}_{2m}^-(2), & \text{when } q \equiv \pm 1 \pmod 8, \end{cases}$$

where $2n = 2^m$. Our theorem in this section is the following.

Theorem 5.6.1 *Let $G \leqslant \mathrm{Sp}_{2n}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. If $G \in \mathcal{C}_6$ then $(n, q) = (2, 3)$ and G is contained in $2_-^{1+4}.\Omega_4^-(2) \cong 2_-^{1+4}.\mathrm{A}_5$.*

Proof. Let M be as above and suppose M contains an element of order $q^n - 1$. Suppose first that $m \geqslant 4$. The largest possible element order in 2_-^{1+2m} is 4 and an upper bound for the element order in $\mathrm{GO}_{2m}^-(2)$ is 2^{m+1}, by Theorem 2.2.6. Therefore

$$q^n - 1 \leqslant 4\left(2^{m+1}\right) = 2^{m+3},$$

and so since q is an odd prime, we have

$$3^n - 1 \leqslant q^n - 1 \leqslant 2^{m+3}.$$

Since $n = 2^m$, there are no integer solutions to this inequality for $m \geqslant 4$ and q an odd prime.

Now suppose that $m = 3$ and so $n = 4$. Then the largest element order in $\mathrm{GO}_6^-(2)$ is 12. Therefore we have

$$80 = 3^4 - 1 \leqslant q^4 - 1 \leqslant 4 \cdot 12 = 48,$$

which cannot happen.

Therefore $m = 2$ and so $n = 2$. The largest element order in $\mathrm{GO}_4^-(2)$ is 6, so this time we get $q^2 - 1 \leqslant 4 \cdot 6 = 24$, which means $q = 3$ or 5. In these cases

$$M \cong 2_-^{1+4}.\Omega_4^-(2) \cong 2_-^{1+4}.\mathrm{A}_5,$$

and the maximum element order in A_5 is 5. This means the largest element order in M is at most $4 \cdot 5 = 20$. But if $q = 5$, then $q^2 - 1 = 24$, so this cannot happen.

Therefore $q = 3$. Letting $\mathfrak{A}$ be the linear Singer subgroup of $\mathrm{Sp}_4(3)$ as usual, we see that $\mathfrak{A}$ has order 8, so is contained in a Sylow 2-subgroup, T of $\mathrm{Sp}_4(3)$. Since M has odd index in $\mathrm{Sp}_4(3)$, M contains a Sylow 2-subgroup, S of $\mathrm{Sp}_4(3)$. Since any two Sylow 2-subgroups are conjugate, there is a $g \in \mathrm{Sp}_4(3)$ such that $S^g = T$. Therefore

$$\mathfrak{A} \leqslant T = S^g \leqslant M^g.$$

This proves the theorem. □

Unitary Case

If $X = \mathrm{GU}_{2n}(q)$, then $q \equiv 3 \bmod 4$ and G lies in

$$M := C_{q+1} \circ 2^{1+2m}.\mathrm{Sp}_{2m}(2),$$

where $2n = 2^m$. Before we prove the main theorem of this section we shall need the following lemma.

Lemma 5.6.2 *For all $d \geqslant 2$, we have the following polynomial factorization*

$$x^{2^d} - 1 = (x+1)(x-1)\prod_{i=1}^{d-1}\left(x^{2^i}+1\right).$$

Proof. We prove by induction on d that

$$\left(x^{2^d} - 1\right)/(x+1) = (x-1)\prod_{i=1}^{d-1}\left(x^{2^i}+1\right).$$

If $d = 2$, we have

$$\left(x^{2^2} - 1\right)/(x+1) = \left(x^2-1\right)\left(x^2+1\right)/(x+1) = (x-1)\left(x^2+1\right),$$

as required, so assume the result for $d = k$. Then by induction, we have

$$\begin{aligned}\left(x^{2^{k+1}} - 1\right)/(x+1) &= \left(x^{2^k}-1\right)\left(x^{2^k}+1\right)/(x+1) \\ &= \left(x^{2^k}+1\right)(x-1)\prod_{i=1}^{k-1}\left(x^{2^i}+1\right) = (x-1)\prod_{i=1}^{k}\left(x^{2^i}+1\right).\end{aligned}$$

Hence result follows by induction. □

Now we are ready to prove the main theorem of this section.

Theorem 5.6.3 *Let $n \geqslant 2$ and $G \leqslant \mathrm{GU}_{2n}(q)$. Suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Then $G \notin \mathcal{C}_6$.*

Proof. Let M be as above. We will show that M cannot contain an element of order $q^{2n} - 1$. Using Theorem 2.2.6, an upper bound for the element order in M is

$$(q+1)\cdot 4 \cdot 2^{m+1} = 2^{m+3}(q+1).$$

If M contained an element of order $q^{2n} - 1$, then $q^{2n} - 1 \leqslant 2^{m+3}(q+1)$ and so

$$\left(q^{2n}-1\right)/\left(q+1\right)\leqslant 2^{m+3}. \tag{5.6.1}$$

Also $2n=2^m$, so by Lemma 5.6.2, we have

$$\begin{aligned}\left(9^n-1\right)/4 &= \left(3^{2n}-1\right)/\left(3+1\right)=\left(3-1\right)\prod_{i=1}^{m-1}\left(3^{2^i}+1\right)\leqslant\left(q-1\right)\prod_{i=1}^{m-1}\left(q^{2^i}+1\right)\\ &= \left(q^{2n}-1\right)/\left(q+1\right)\end{aligned}$$

and so $\left(9^{2^{m-1}}-1\right)/4\leqslant 2^{m+3}$. This inequality gives only the solution $m=2$. In this case, we also have $n=2$ and so since $q\equiv 3 \bmod 4$, Inequality 5.6.1 gives only the solution $q=3$. Therefore

$$M=4\circ 2^{1+4}\mathrm{Sp}_4\left(2\right)\cong 4\circ 2^{1+4}\mathrm{S}_6$$

lying inside $\mathrm{GU}_4\left(3\right)$. But the largest element order in $4\circ 2^{1+4}$ and S_6 are 4 and 6, respectively, and so the largest possible element order in M is 24. Since $q^{2n}-1=80$, we have a contradiction. This concludes the proof of the theorem. □

Orthogonal Case

If $X=\mathrm{GO}_{2n}^{+}\left(q\right)$, then q is an odd prime and G is contained in

$$M:=\begin{cases}2_{+}^{1+2m}.\Omega_{2m}^{+}\left(2\right), & \text{if } q\equiv\pm 3 \bmod 8,\\ 2_{+}^{1+2m}.\mathrm{GO}_{2m}^{+}\left(2\right), & \text{if } q\equiv\pm 1 \bmod 8,\end{cases}$$

where $2n=2^m$. Our main theorem in this section is as follows.

Theorem 5.6.4 *Let $n\geqslant 3$ and $G\leqslant\mathrm{GO}_{2n}^{+}\left(q\right)$. Suppose that G contains a linear Singer cycle of $\mathrm{GO}_{2n}^{+}\left(q\right)$. Then $G\notin\mathcal{C}_6$.*

Proof. Let M be as above. We show that M cannot contain any element of order q^n-1.

If $m \geqslant 4$, then an upper bound for the element order in $\mathrm{GO}^{+}_{2m}(2)$ is 2^{m+1}, using Theorem 2.2.6. Following the same method as in the symplectic case then gives a contradiction.

So we can assume $m = 3$, which means $n = 4$. Using MAGMA [5] the maximum element order in $\mathrm{GO}^{+}_{6}(2)$ is 15, so we have

$$q^4 - 1 \leqslant 4 \cdot 15 = 60$$

But this has no solutions for q an odd prime. Therefore M cannot contain any element of order $q^n - 1$ and so the result follows. □

5.7 Tensor induced subgroups

Now we can assume that G is contained in $\mathcal{C}_7$. This means that G preserves a tensor product decomposition of the form $V = \bigotimes_{i=1}^{m} V_i$, where $\dim(V_i) = k$. We will show that for all possibilities for X, these groups do not contain linear Singer cycles of X. We will use primitive prime divisors of $q^{un} - 1$ to rule out all cases except the case when $X = \mathrm{GU}_4(q)$ and $(k, m) = (2, 2)$. In this case, we apply the element order bounds from Theorem 2.2.6 to prove the result.

Symplectic Case

First, let $X = \mathrm{Sp}_{2n}(q)$. Then $2n = (2k)^m$ and G is contained in the group

$$M := 2.\left(\mathrm{PSp}_{2k}(q).2 \wr \mathrm{S}_m\right)\frac{1}{2},$$

where qm is odd. Our theorem in this section is the following.

Theorem 5.7.1 *Let $n \geqslant 2$ and $G \leqslant \mathrm{Sp}_{2n}(q)$. If G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$, then $G \notin \mathcal{C}_7$.*

Proof. Let M be as above with $2n = (2k)^m$ and qm odd. We will show that the order of M cannot be divisible by a primitive prime divisor of $q^n - 1$ and so M cannot contain a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$.

We know qm is odd, so $q^n - 1$ has a primitive prime divisor. If r is such a prime divisor and r divides $|M|$, then r must divide the order of $\mathrm{Sp}_{2k}(q) \wr \mathrm{S}_m$.

Now, r is a primitive prime divisor, so we have

$$r \geqslant n + 1 > (2k)^m / 2 \geqslant m.$$

Hence r cannot divide the order of S_m, therefore r divides the order of $\mathrm{Sp}_{2k}(q)$. This means that r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant k$. This cannot happen as $2k < (2k)^m / 2 = n$. The result follows. □

Unitary Case

Now let $X = \mathrm{GU}_{2n}(q)$. In this case $2n = k^m$ and G is contained in the group

$$M := C_{q+1}.\left(\mathrm{PGU}_k(q) \wr \mathrm{S}_m\right).$$

Our main theorem is the following.

Theorem 5.7.2 *Let $n \geqslant 2$ and $G \leqslant \mathrm{GU}_{2n}(q)$. If G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, then $G \notin \mathcal{C}_7$.*

Proof. Let M be as above with $2n = k^m$. We will show that M cannot contain any element of order $q^{2n} - 1$.

First assume $(k, m) \neq (2, 2)$. Since $2n = k^m > 4$, $q^{2n} - 1$ has a primitive prime divisor, r. If M contains an element of order $q^{2n} - 1$, then its order is divisible by r. Now r cannot divide $q+1$, since $n \geqslant 2$ and since r is a primitive prime divisor, we have

$$r \geqslant 2n+1 = k^m + 1 > m,$$

so r cannot divide $|\mathrm{S}_m|$. Hence, r divides $|\mathrm{PGU}_k(q)|$, so divides an expression of the form $q^i - (-1)^i$, for $2 \leqslant i \leqslant k$. But since $(k,m) \neq (2,2)$, we have $2k < 2n$, which cannot happen.

Therefore $(k,m) = (2,2)$, and so $n = 2$ and M becomes

$$C_{q+1}.\left(\mathrm{PGU}_2(q) \wr 2\right) \cong C_{q+1}.\left(\mathrm{PGL}_2(q) \wr 2\right).$$

By Theorem 2.2.6, an upper bound on the element order of M is $2(q+1)^3$ and so we get, $q^4 - 1 \leqslant 2(q+1)^3$, which yields $q = 2$ or $q = 3$. But in these cases, $q^4 - 1$ is divisible by 5, which does not divide the order of M.

We therefore conclude that M does not contain any element of order $q^{2n} - 1$. □

Orthogonal Case

Finally, let $X = \mathrm{GO}^+_{2n}(q)$. Then $2n = (2k)^m$ and either G is contained in the group

$$2.\left(\mathrm{PSp}_{2k}(q).2 \wr \mathrm{S}_m\right)\frac{1}{2},$$

where kq is even, or G is contained in the group

$$2.\left(\mathrm{PGO}^{\pm}_{2k}(q).2 \wr \mathrm{S}_m\right)\frac{1}{2},$$

where q is odd. Our main theorem is the following.

Theorem 5.7.3 *Let $n \geqslant 3$ and $G \leqslant \mathrm{GO}^+_{2n}(q)$. If G contains a linear Singer cycle of $\mathrm{GO}^+_{2n}(q)$, then $G \notin \mathcal{C}_7$.*

We will show that the orders of the above groups in $\mathcal{C}_7$ are not divisible by primitive prime divisors of $q^n - 1$, then Theorem 5.7.3 will follow.

Proposition 5.7.4 *Suppose that* $2n = (2k)^m$ *and* kq *is even. Then the order of*

$$M := 2.\left(\mathrm{PSp}_{2k}\left(q\right).2 \wr \mathrm{S}_m\right)\frac{1}{2}$$

is not divisible by a primitive prime divisor of $q^n - 1$.

Proof. Because $m \geqslant 2$, we have $n > 3$. Therefore a primitive prime divisor of $q^n - 1$ exists. Now argue as in Theorem 5.7.1. □

Proposition 5.7.5 *Suppose that* $2n = (2k)^m$ *and* q *is odd. Then the order of*

$$M := 2.\left(\mathrm{PGO}^{\pm}_{2k}\left(q\right).2 \wr \mathrm{S}_m\right)\frac{1}{2}$$

is not divisible by a primitive prime divisor of $q^n - 1$.

Proof. Since $n \geqslant 3$ and q is odd, $q^n - 1$ does indeed have a primitive prime divisor. Let r be a primitive prime divisor of $q^n - 1$ and assume that r divides the order of M. Then r must divide the order of $\mathrm{GO}^{\pm}_{2k}\left(q\right) \wr \mathrm{S}_m$. By the same argument as in Theorem 5.7.1, we see that r cannot divide $|\mathrm{S}_m|$ and so divides $\left|\mathrm{GO}^{\pm}_{2m}\left(q\right)\right|$ Hence either r divides $q^m \mp 1$, or r divides an expression of the form $q^{2i} - 1$, for $1 \leqslant i \leqslant m - 1$. Both of these possibilities give a contradiction, since $2m < n$. □

Proposition 5.7.4 and 5.7.5 together prove Theorem 5.7.3.

5.8 Classical subgroups

Finally we can now assume that G is contained in the class $\mathcal{C}_8$ of classical groups embedded in X. These groups only occur when $X = \mathrm{Sp}_{2n}\left(q\right)$ and q is even and consist of the subgroups $\mathrm{GO}^{\pm}_{2n}\left(q\right)$. Our final main theorem of this chapter is the following.

Theorem 5.8.1 *Let $n \geqslant 2$ and $G \leqslant \mathrm{Sp}_{2n}(q)$. Also assume that G contains a linear Singer cycle of* $\mathrm{Sp}_{2n}(q)$ *and suppose that $G \in \mathcal{C}_8$, so q is even. Then G is contained in* $\mathrm{GO}^{+}_{2n}(q)$.

The discussion preceding Proposition 3.2.9 shows that the linear Singer cycle of $\mathrm{Sp}_{2n}(q)$ preserves a quadratic form of plus type on V. Therefore, the linear Singer cycle of $\mathrm{Sp}_{2n}(q)$ is contained in $\mathrm{GO}^{+}_{2n}(q)$. However the subgroups $\mathrm{GO}^{-}_{2n}(q)$ do not contain a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. This a result of the following proposition.

Proposition 5.8.2 *Let $\mathfrak{A}$ be the linear Singer subgroup of* $\mathrm{Sp}_{2n}(q)$. *If $\mathfrak{A}$ preserves a quadratic form on the vector space V, then it has plus type.*

Proof. Let Q be a quadratic form on V which is preserved by $\mathfrak{A}$ and let U be a proper non-zero $\mathfrak{A}$-invariant subspace of V. Note that U has dimension n by Theorem 3.2.2. By Aschbacher [3, the proofs of 20.11, 21.1, 21.2 and 21.3], U contains a singular vector. Since $\mathfrak{A}$ is transitive on non-zero vectors of U and $\mathfrak{A}$ preserves Q, all vectors in U are singular and hence, all vectors are isotropic. This means U is a totally singular subspace. We conclude that the Witt index of Q is n and so Q has plus type. □

This concludes the classical subgroups case and the geometric case.

Chapter 6

Almost simple cases

In this chapter, we assume a subgroup G of X containing a linear Singer cycle of X lies in class $\mathcal{S}$ of Aschbacher's Theorem. Recall that $G \in \mathcal{S}$ if and only if the following hold:

a) The socle of G is a non-abelian simple group, S, so that

$$S \leqslant G/\left(G \cap \mathrm{Z}\left(X\right)\right) \leqslant \mathrm{Aut}\left(\mathrm{S}\right).$$

b) If L is the full covering group of S and $\rho : L \to \mathrm{GL}_{2n}\left(q^u\right)$ is a representation of L corresponding to G, in the sense that $\rho\left(L\right) \leqslant G$ and

$$\rho\left(L\right) / \left(\rho\left(L\right) \cap \mathrm{Z}\left(X\right)\right) \cong S,$$

then $\rho\left(L\right)$ is absolutely irreducible.

c) $\rho\left(L\right)$ cannot be realized over a proper subfield of $\mathrm{GF}\left(q^u\right)$.

d) If $\rho\left(L\right)$ preserves a non-degenerate quadratic form on V, then $X_0 = \Omega_{2n}^{+}\left(q\right)$.

e) If $\rho\left(L\right)$ preserves a non-degenerate symplectic form but no non-degenerate quadratic form on V, then $X_0 = \mathrm{Sp}_{2n}\left(q\right)$.

f) If $\rho(L)$ preserves a non-degenerate unitary form on V, then $X_0 = \mathrm{SU}_{2n}(q)$.

We note that, if $\mathfrak{A}$ is the linear Singer subgroup of X as usual, then since $\mathfrak{A}$ contains the centre of X, we have $\mathrm{Z}(X) \leqslant \mathrm{Z}(X) \cap G$. On the other hand, $\mathrm{Z}(X) \cap G \leqslant \mathrm{Z}(X)$, so in fact $\mathrm{Z}(X) \cap G = \mathrm{Z}(X)$.

In the following four sections, we will determine possibilities for G by considering each of the possible cases for S. Using the Classification of Finite Simple Groups, we consider the cases when S is an alternating group, a sporadic group, and a Lie-type group. We consider separately the cases where a Lie type group is defined over a field of characteristic dividing q and coprime to q.

We first deal with the sporadic groups.

6.1 Sporadic groups

Assume that S is one of the twenty six sporadic simple groups. The maximum element orders in $\mathrm{Aut}(S)$ are known and can be found by looking at the character tables of S given in the Atlas [9]. Let $\overline{X}$ denote $X/\mathrm{Z}(X)$. The image of the linear Singer cycle of X in $\overline{X}$ has order $(q^{un}-1)/d$ where

$$d = \begin{cases} q+1, & \text{if } X = \mathrm{GU}_{2n}(q), \\ \gcd(2, q-1), & \text{otherwise.} \end{cases}$$

So if G lies in $\mathcal{S}$ and contains a linear Singer cycle then, using $\mathrm{meo}(H)$ to denote the maximum element order in a group H, we have

$$(q^{un}-1)/d \leqslant \mathrm{meo}(\mathrm{Aut}(S)). \tag{6.1.1}$$

Also we use a paper by Jansen [20], which lists the minimal representation degrees for all the sporadic simple groups and their covering groups. From this, we can deduce the

S	$\mathrm{meo}(\mathrm{Aut}(S))$	$\mathrm{R}(S)$	S	$\mathrm{meo}(\mathrm{Aut}(S))$	$\mathrm{R}(S)$
M_{11}	11	5	He	42	50
M_{12}	12	6	Ly	67	111
M_{22}	14	6	O′N	56	45
M_{23}	23	11	Co_1	60	24
M_{24}	23	11	Co_2	30	22
J_1	19	7	Co_3	30	22
J_2	24	6	Fi_{22}	42	27
J_3	34	9	Fi_{23}	60	253
J_4	66	112	Fi'_{24}	84	781
HS	30	20	HN	60	132
Suz	40	12	Th	39	248
McL	30	21	$\mathbb{B}$	70	4370
Ru	29	28	$\mathbb{M}$	119	196882

Table 6.1: $\mathrm{meo}(\mathrm{Aut}(S))$ and $\mathrm{R}(S)$, where S is a sporadic group.

minimal projective representation degrees of a sporadic group. Since S is embedded into $\overline{X}$, it has a projective representation of degree $2n$. So, using $\mathrm{R}(H)$ to denote the minimal projective representation degree of a group H, we have

$$n \geqslant \frac{1}{2}\mathrm{R}(S). \tag{6.1.2}$$

Using Inequalities 6.1.1 and 6.1.2 gives us an easy way to rule out most of the possibilities for S. We shall see that there are no cases for S if G lies in $\mathcal{S}$ and contains a linear Singer cycle. For convenience, the values for $\mathrm{meo}(\mathrm{Aut}(S))$ and $\mathrm{R}(S)$ are given in Table 6.1. We shall use this method throughout this chapter, as well as using results from Hiss [17] and Lübeck [26] to rule out values of n. Our main result is the following.

Theorem 6.1.1 *Let G be a subgroup of X lying in $\mathcal{S}$ such that $G/\mathrm{Z}(X)$ has socle S where S is one of the* 26 *sporadic simple groups. Then G does not a contain linear Singer cycle*

Proof. Suppose that G contained a linear Singer cycle. Assume first that $X = \mathrm{GU}_{2n}(q)$. Then Inequality 6.1.1 becomes

$$\left(q^{2n} - 1\right) / (q + 1) \leqslant \mathrm{meo}\left(\mathrm{Aut}\left(S\right)\right)$$

and so using this together with Inequality 6.1.2 and the values in Table 6.1, we can reduce to the case when $S = \mathrm{J}_2$ and $(n, q) = (3, 2)$. Hence we get an embedding of J_2 in $\mathrm{PGU}_6(2)$. But this cannot happen since 25 divides the order of J_2 but not the order of $\mathrm{PGU}_6(2)$.

Therefore we can assume that X is either $\mathrm{Sp}_{2n}(q)$ or $\mathrm{GO}^{+}_{2n}(q)$. Inequality 6.1.1 then becomes

$$(q^n - 1) / \gcd(2, q - 1) \leqslant \mathrm{meo}\left(\mathrm{Aut}\left(S\right)\right).$$

Again, using this with Inequality 6.1.2 and Table 6.1, we can reduce to the following cases:

i) $S = \mathrm{M}_{11}$ and $(n, q) = (3, 2)$,

ii) $S = \mathrm{M}_{12}$ and $(n, q) = (3, 2)$

iii) $S = \mathrm{M}_{22}$ and $(n, q) = (3, 2)$ or $(3, 3)$,

iv) $S = \mathrm{J}_1$ and $(n, q) = (4, 2)$,

v) $S = \mathrm{J}_2$ and $(n, q) = (3, 2)$, $(3, 3)$, or $(4, 2)$,

vi) $S = \mathrm{J}_3$ and $(n, q) = (5, 2)$.

We can rule out most of these cases as these would contradict Jansen's result. For instance, M_{11} has no 6-dimensional faithful irreducible representation in characteristic 2, so we cannot have $S = \mathrm{M}_{11}$ and $(n, q) = (3, 2)$. The only cases we have to consider are when $S = \mathrm{J}_2$ and $(n, q) = (3, 2)$, $(3, 3)$ or $(4, 2)$. The last case is ruled out since J_2 has no 8-dimensional faithful irreducible representation in characteristic 2 by [17]. Hence J_2 embeds in $\mathrm{PSp}_6(2)$, $\mathrm{PSp}_6(3)$ or $\mathrm{PGO}_6^+(3)$. But 25 divides the order of J_2 but not the order of these groups.

Therefore since we have exhausted all possibilities for S, we can conclude that G cannot contain a linear Singer cycle of X. □

6.2 Alternating groups

We now assume that S is an alternating group on k letters where $k \geqslant 5$. Results of Dickson and Wagner [10, 33, 34] give the smallest irreducible representation degrees of A_k. Together with [35], we can deduce the minimal irreducible projective representation degrees of A_k. From [24, 5.3.7], if $k \geqslant 9$, then $\mathrm{R}(A_k) = k - 2$. If $5 \leqslant k \leqslant 8$ then $\mathrm{R}(A_k)$ is smaller than $k - 2$. For this reason, we divide the case of the Alternating groups into these two cases.

For $5 \leqslant k \leqslant 8$, we use the same approach as in the sporadic case. If G lies in $\mathcal{S}$ and has socle A_k, we use Inequalities 6.1.1 and 6.1.2 to find values for n and q, then we examine whether G can contain a linear Singer cycle of X. For $k \geqslant 9$, we will use primitive prime divisors which we will also use throughout the rest of this chapter.

Theorem 6.2.1 *Let G be a subgroup of X containing a linear Singer cycle of X. Also suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is A_k where $5 \leqslant k \leqslant 8$. Then either $X = \mathrm{Sp}_4(2)$ and $G = \mathrm{A}_6$, or $X = \mathrm{GO}_6^+(2)$ and $\mathrm{A}_7 \leqslant G \leqslant \mathrm{S}_7$.*

Proof. First let $X = \mathrm{GU}_{2n}(q)$, so the image of the linear Singer cycle of X in $\overline{X}$ has order $(q^{2n} - 1) / (q + 1)$. By our assumptions, we have

$$\left(q^{2n} - 1\right) / (q + 1) \leqslant \mathrm{meo}(\mathrm{Aut}(\mathrm{A}_k)) \leqslant \mathrm{meo}(\mathrm{S}_8) = 15.$$

The only integer solution to this inequality with $n \geqslant 2$ and q a power of a prime is $(n, q) = (2, 2)$. Then we have an embedding of A_k in $\mathrm{PGU}_4\,(2)$. This immediately rules out $k = 7$ and $k = 8$, as in these cases 7 divides the order of A_k but not the order of $\mathrm{PGU}_4\,(2)$. Now in $\mathrm{PGU}_4\,(2)$, there are two conjugacy classes of groups isomorphic to A_5 contained in a single conjugacy class of A_6 from MAGMA [5]. But these are contained in the group $\mathrm{Sp}_4\,(2)$ which is a member of $\mathcal{C}_5$.

This completes the case when $X = \mathrm{GU}_{2n}\,(q)$, so we may assume that X is either $\mathrm{Sp}_{2n}\,(q)$ or $\mathrm{GO}^+_{2n}\,(q)$. This time the image of the linear Singer cycle of X in $\overline{X}$ has order $(q^n - 1) \,/\, \gcd\,(2, q-1)$.

We now consider each value of k separately. Suppose first that $S = \mathrm{A}_5$. Then using Inequality 6.1.1, we get

$$(q^n - 1) \,/\, \gcd\,(2, q-1) \leqslant \mathrm{meo}\,(\mathrm{S}_5) = 6.$$

The only integer solutions to this inequality with $n \geqslant 2$ and q a power of a prime are $(n, q) = (2, 2)$ or $(2, 3)$. Since we are assuming that $n \geqslant 3$ when $X = \mathrm{GO}^+_{2n}\,(q)$, we only need to consider $\overline{X} = \mathrm{Sp}_4\,(2)$ or $\mathrm{PSp}_4\,(3)$. If $\overline{X} = \mathrm{Sp}_4\,(2)$, then there are two conjugacy classes of subgroups isomorphic to A_5 in $\overline{X}$, using MAGMA [5]. One class has representative $\mathrm{Sp}_2\,(4)$ which is a member of $\mathcal{C}_3$, the other has representative $\mathrm{GO}^-_4\,(2)$ which is a member of $\mathcal{C}_8$. So $\overline{X} = \mathrm{PSp}_4\,(3)$. In this case, there are also two conjugacy classes of groups isomorphic to A_5 in $\overline{X}$, but they are both contained in a conjugate of $\mathrm{PSp}_2\,(9)$ which is a member of $\mathcal{C}_3$.

If $S = \mathrm{A}_6$, then Inequality 6.1.1 gives

$$(q^n - 1) \,/\, \gcd\,(2, q-1) \leqslant \mathrm{meo}\,(\mathrm{P\Gamma L}_2\,(9)) = 10.$$

The only integer solutions to this inequality with $n \geqslant 2$ and q a power of a prime are $(n,q) = (2,2), (2,3)$ or $(3,2)$. We can immediately ignore $(n,q) = (3,2)$, as then $(q^n - 1) / \gcd(2, q-1) = 7$, which does not divide the order of $\mathrm{P\Gamma L}_2(9)$. Therefore by our assumptions, we have either $\overline{X} = \mathrm{Sp}_4(2)$ or $\mathrm{PSp}_4(3)$. If $\overline{X} = \mathrm{PSp}_4(3)$. Then there is a single conjugacy class of subgroups isomorphic to A_6 in $\overline{X}$. But any representative of this class is conjugate to $\mathrm{PSp}_2(9)$ which lies in $\mathcal{C}_3$. Therefore $\overline{X} = \mathrm{Sp}_4(2)$. Now A_6 is a normal subgroup of $\mathrm{Sp}_4(2)$ lying in $\mathcal{S}$ and the linear Singer cycle of $\mathrm{Sp}_4(2)$ has order 3. Moreover, via the isomorphism $\mathrm{Sp}_4(2) \cong \mathrm{S}_6$, all element of order 3 in $\mathrm{Sp}_4(2)$ correspond to even permutations in S_6. Therefore the linear Singer cycle of $\mathrm{Sp}_4(2)$ is contained in A_6. Therefore we have

$$\mathrm{A}_6 \leqslant G/\mathrm{Z}(G) \cong G \leqslant \mathrm{Sp}_4(2).$$

Since G is a proper subgroup of $\mathrm{Sp}_4(2)$, G is conjugate to A_6.

If $S = \mathrm{A}_7$, then Inequality 6.1.1 gives

$$(q^n - 1) / \gcd(2, q-1) \leqslant \mathrm{meo}(\mathrm{S}_7) = 12.$$

The only integer solutions to this inequality with $n \geqslant 2$ and q a power of a prime are $(n,q) = (2,2), (2,3), (2,5)$ or $(3,2)$. If $(n,q) \neq (3,2)$, then $\overline{X}$ is one of $\mathrm{Sp}_4(2), \mathrm{PSp}_4(3)$ or $\mathrm{PSp}_4(5)$. But 7 does not divide the order of $\overline{X}$, so A_7 cannot embed in $\overline{X}$. So $(n,q) = (3,2)$ and $\overline{X} = \mathrm{Sp}_6(2)$ or $\mathrm{GO}_6^+(2)$. Now in $\mathrm{GO}_6^+(2)$, the linear Singer cycle has order 7 and all subgroups of order 7 in $\mathrm{GO}_6^+(2)$ are conjugate. Also using MAGMA [5] and [6, Table 8.3.2], there is a single conjugacy class of subgroups isomorphic to S_7 lying in $\mathcal{S}$ and these contain an element of order 7. Therefore the linear Singer cycle of $\mathrm{GO}_6^+(2)$ is contained in a conjugate of S_7. Therefore since $G/\mathrm{Z}(X)$ is almost simple, we have $\mathrm{A}_7 \leqslant G \leqslant \mathrm{S}_7$. As a consequence of this, we can see there is a single conjugacy class of subgroups isomorphic to S_7 in $\mathrm{Sp}_6(2)$, but this is contained in $\mathcal{C}_8$.

Finally, If $S = \mathrm{A}_8$, then Inequality 6.1.1 gives

$$(q^n - 1) / \gcd(2, q-1) \leqslant \mathrm{meo}(\mathrm{S}_8) = 15.$$

The only integer solutions to this inequality with $n \geqslant 2$ and q a power of a prime are $(n, q) = (2,2), (2,3), (2,4), (2,5), (3,2), (3,3)$ or $(4,2)$. If $n = 2$, then $\overline{X} = \mathrm{PSp}_4(q)$. But for these values of q, 7 divides the order of A_8 but not the order of $\overline{X}$. If $(n,q) = (3,3)$, then $\overline{X} = \mathrm{PSp}_6(3)$ or $\mathrm{PGO}_6^+(3)$. In both these cases, the image of the linear Singer cycle in $\overline{X}$ has order 13, which doesn't divide the order of S_8, so these cases are also ruled out. If $(n,q) = (3,2)$, then $\overline{X} = \mathrm{Sp}_6(2)$ or $\mathrm{GO}_6^+(2)$. In the latter case, there is a single conjugacy class of subgroups isomorphic to A_8. But as $\mathrm{A}_8 \cong \Omega_6^+(2)$, this contradicts our assumptions on G. This also means that the single conjugacy class of subgroups isomorphic to A_8 in $\mathrm{Sp}_6(2)$ are contained in $\mathcal{C}_8$, so we can ignore this case. This leaves us with the case when $(n,q) = (4,2)$. Here $\overline{X} = \mathrm{Sp}_8(2)$ or $\mathrm{GO}_8^+(2)$. But by [17], there are no 8-dimensional absolutely irreducible representations of A_8 in characteristic 2.

This concludes the proof of the theorem. □

We can now assume $k \geqslant 9$.

Theorem 6.2.2 *Let G be a subgroup of X lying in $\mathcal{S}$ such that the socle of $G/\mathrm{Z}(X)$ is A_k for $k \geqslant 9$. Then $X = \mathrm{GO}_8^+(2)$ and $G = \mathrm{A}_9$.*

Proof. In this case $\mathrm{Aut}(\mathrm{A_k}) = \mathrm{S_k}$. By [24, 5.3.7], the minimal degree for an irreducible projective representation of A_k is $k-2$, so $k \leqslant 2n+2$ and $G/\mathrm{Z}(X) \leqslant \mathrm{S_{2n+2}}$.

Note that $k \geqslant 9$ implies that $n \geqslant 4$. If $(n,q,u) = (6,2,1)$, then $(q^{un} - 1)/d = 63$. But then $G/\mathrm{Z}(X) \leqslant \mathrm{S}_{14}$ and S_{14} contains no element of this order since it would have to contain in its disjoint cycle decomposition: a cycle of length 63, or a cycle of length 7 and a cycle of length 9.

Therefore, $q^{un}-1$ has a primitive prime divisor. Let r be such a primitive prime divisor and let a be the image of the linear Singer cycle in $G/\mathrm{Z}(X)$. Also let $(l_1,\ldots,l_m)$ be the lengths of the cycles in the disjoint cycle decomposition of a. Since the order of a is the least common multiple of the lengths of its disjoint cycles, r divides l_i for some i and so $r \leqslant 2n+2$. On the other hand, by Remark 2.2.3, we have

$$r = \begin{cases} 2xn+1, & \text{if } X = \mathrm{GU}_{2n}(q), \\ xn+1, & \text{otherwise,} \end{cases}$$

for some $x \in \mathbb{N}$. Therefore, we either have $r = 2n+1$, or $X \neq \mathrm{GU}_{2n}(q)$ and $r = n+1$.

If $r = 2n+1$, then since r divides l_i and $l_i \leqslant 2n+2$, we see that a is a cycle of length $2n+1$ and therefore $(q^{un}-1)/d = 2n+1$. But there are no integer solutions to this equation with $n \geqslant 4$ and q a power of a prime.

Therefore $X \neq \mathrm{GU}_{2n}(q)$, $u = 1$ and $r = n+1$. Suppose r^2 divides q^n-1. If r^2 divides one of the l_i, then this would mean that

$$r^2 = n^2+2n+1 \leqslant 2n+2,$$

which gives $n^2 \leqslant 1$, contrary our assumptions. Hence r must divide l_i and l_j with $i \neq j$ and so a is the product of two cycles of length $n+1$, which yields $(q^n-1)/d = n+1$. But again, this has no integer solutions to this equation with $n \geqslant 4$ and q a prime power.

It follows that r^2 does not divide q^n-1. Therefore, r is a small primitive prime divisor of q^n-1 and so by Theorem 2.2.5, this leaves only the following possibilities to consider:

i) $q = 2$ and $n \in \{4, 10, 12, 18\}$,

ii) $q = 3$ and $n \in \{4, 6\}$,

iii) $(q, n) = (5, 6)$.

If $(n, q) = (10, 2), (18, 2)$, or $(6, 5)$, then $(q^n - 1)/d$ does not divide the order of S_{2n+2}, so these cases are automatically ruled out. If $(n, q) = (4, 3)$, then $(q^n - 1)/d = 40 = 2^3 \cdot 5$ so any element of this order would need to act on at least $8 + 5 = 13$ points. Therefore $a \notin \mathrm{S}_{10}$ in this case. If $(n, q) = (6, 3)$, then

$$(q^n - 1)/d = 364 = 2^2 \cdot 7 \cdot 13.$$

Any element of this order would need to act on at least $4 + 7 + 13 = 24$ points and so $a \notin \mathrm{S}_{14}$. Also if $(n, q) = (12, 2)$, then

$$(q^n - 1)/d = 1023 = 3^2 \cdot 5 \cdot 7 \cdot 13,$$

so any element of this order would need to act on at least $9 + 5 + 7 + 13 = 34$ points. Therefore $a \notin \mathrm{S}_{26}$.

This leaves the case when $(n, q) = (4, 2)$. Here we have $G \cong G/\mathrm{Z}(X) \leqslant \mathrm{S}_{10}$ and $k = 9$ or 10. If $k = 9$, then up to conjugacy, there are two subgroups of $\mathrm{GO}_8^+(2)$ isomorphic to A_9 lying in $\mathcal{S}$, from MAGMA [5], [6, Table 8.50] and the ATLAS [9, p. 85]. One of these is contained in a subgroup isomorphic to S_9, the other is not. As mentioned in the proof of Proposition 5.4.4, up to conjugacy, there are two subgroups of order 15 in $\mathrm{GO}_8^+(2)$, only one of which is self-centralizing. From Appendix A.2, the copy of A_9 lying in S_9 contains a non-self-centralizing subgroup of order 15, whereas the copy of A_9 that is not contained in S_9 contains a self-centralizing subgroup of order 15. Hence, the linear Singer cycle of $\mathrm{GO}_8^+(2)$ is contained in a conjugate of this latter subgroup. Therefore, since G is almost simple, we have $G = \mathrm{A}_9$. Now in $\mathrm{Sp}_8(2)$, there are two conjugacy classes of subgroups isomorphic to A_9. But these are contained in a member of $\mathcal{C}_8$.

So $k = 10$. From MAGMA [5], there are no subgroups of $\mathrm{GO}_8^+(2)$ having the same order as A_{10}, so this case is ruled out. Also from MAGMA [5] and [6, Table 8.49], up to conjugacy, there is a subgroup of $\mathrm{Sp}_8(2)$ isomorphic to A_{10} contained in a maximal subgroup isomorphic to S_{10}. As shown in Appendix A.3, up to conjugacy, there are three subgroups of order 15 in $\mathrm{Sp}_8(2)$, only one of which is self-centralizing. However, the subgroup of order 15 in S_{10} is not self-centralizing in $\mathrm{Sp}_8(2)$ and so cannot be conjugate to the linear Singer subgroup of $\mathrm{Sp}_8(2)$.

This conclude the proof of the theorem and the alternating case. □

6.3 Lie-type groups in non-defining characteristic

We can now assume that S is a simple group of Lie-type. We first consider the case when S is defined over the field $\mathrm{GF}(s)$, where p does not divide s. In this section we will prove the following theorem.

Theorem 6.3.1 *Let G be a subgroup of X containing a linear Singer cycle of X. Also suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is a simple group of Lie-type defined over a field whose characteristic does not divide q. Then either $X = \mathrm{Sp}_6(2)$ and*

$$\mathrm{PSU}_3(3) \leqslant G \leqslant \mathrm{PSU}_3(3) : 2,$$

or $X = \mathrm{Sp}_6(3)$ and G is one of two copies of $\mathrm{SL}_2(13)$.

To prove this, we will make use of results of Landazuri and Seitz [25], which give lower bounds on the minimal degree of a projective representation of a Lie-type group in non-defining characteristic. These are illustrated in Table 6.2 which we have taken from [24, Theorem 5.3.9]. Here $e(S)$ denotes a lower bound for the minimum projective representation degree of S in characteristic coprime to p.

We follow a similar approach to the method of Guralnick et al [15, Proposition 8.1]. If $q^{un} - 1$ has a primitive prime divisor, we use a result of Hering [16], which gives the largest prime dividing the order of a Lie-type group, to rule out all but a few finite and

S	$e(S)$	exceptions
$\mathrm{PSL}_2(s)$	$(s-1)/(2,s-1)$	$e(\mathrm{PSL}_2(4))=2$ $e(\mathrm{PSL}_2(9))=3$
$\mathrm{PSL}_k(s), k \geqslant 3$	$s^{k-1}-1$	$e(\mathrm{PSL}_3(2))=2$ $e(\mathrm{PSL}_3(4))=4$
$\mathrm{PSp}_{2k}(s), k \geqslant 2$	$\left(s^k-1\right)/2, s$ odd $s^{k-1}\left(s^{k-1}-1\right)(s-1)/2, s$ even	$e\left(\mathrm{PSp}_4(2)'\right)=2$ $e(\mathrm{PSp}_6(2))=7$
$\mathrm{PSU}_k(s), k \geqslant 3$	$s\left(s^{k-1}-1\right)/(s+1)$, k odd $\left(s^k-1\right)/(s+1)$, k even	$e(\mathrm{PSU}_4(2))=4$ $e(\mathrm{PSU}_4(3))=6$
$\mathrm{P}\Omega_{2k}^{+}(s), k \geqslant 4$	$\left(s^{k-1}-1\right)\left(s^{k-2}+1\right)$, $s \neq 2,3,5$ $s^{k-2}\left(s^{k-1}-1\right)$, $s=2,3,5$	 $e(\mathrm{P}\Omega_8(2))=8$
$\mathrm{P}\Omega_{2k}^{-}(s), k \geqslant 4$	$\left(s^{k-1}+1\right)\left(s^{k-2}-1\right)$	
$\Omega_{2k+1}(s), k \geqslant 3, s$ odd	$s^{2(k-1)}-1, s>5$ $s^{k-1}\left(s^{k-1}-1\right), s=3,5$	$e(\Omega_7(3))=27$
$\mathrm{E}_6(s), {}^2\mathrm{E}_6(s)$	$s^9(s^2-1)$	
$\mathrm{E}_7(s)$	$s^{15}(s^2-1)$	
$\mathrm{E}_8(s)$	$s^{27}(s^2-1)$	
$\mathrm{F}_4(s)$	$s^6(s^2-1), s$ odd $s^7(s^3-1)(s-1)/2, s$ even	 $e(\mathrm{F}_4(2)) \geqslant 44$
$\mathrm{G}_2(s)$	$s(s^2-1)$	$e(\mathrm{G}_2(3))=14$ $e(\mathrm{G}_2(4))=12$
${}^3\mathrm{D}_4(s)$	$s^3(s^2-1)$	
${}^2\mathrm{F}_4(s)$, $s=2^{2m+1}$	$s^4\sqrt{s/2}(s-1)$	
${}^2\mathrm{B}_2(s)$, $s=2^{2m+1}$	$\sqrt{s/2}(s-1)$	$e({}^2\mathrm{B}_2(8))=8$
${}^2\mathrm{G}_2(s)$, $s=3^{2m+1}$	$s(s-1)$	

Table 6.2: Lower bounds for the minimal degree of projective representations of Lie type groups in non-defining characteristic.

infinite cases. We then deal with these separately using Theorem 2.2.6 as well as MAGMA and the ATLAS [5, 9].

But before we can do this, we need to deal with the case when $q^{un}-1$ has no primitive prime divisors.

Proposition 6.3.2 *Let G be a subgroup of X and suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is a simple group of Lie-type defined over a field whose characteristic does not divide q. If $q^{un}-1$ does not have a primitive prime divisor, then G does not contain a linear Singer cycle of X.*

Proof. Suppose that G does contain a linear Singer cycle of X. By Theorem 2.2.2 and our assumptions on n, if $q^{un}-1$ has no primitive prime divisor, then either $(n,q)=(6/u,2)$ or $X=\mathrm{Sp}_{2n}(q)$ and $n=2$. Suppose first that $(n,q)=(6/u,2)$. If $X\neq \mathrm{GU}_{2n}(q)$, then we have a 12-degree projective representation in characteristic 2. Thus s is odd and $e(S)\leqslant 12$. By examining the possible values of $e(S)$ in Table 6.2, the only cases when we get integer solutions to this inequality are when

1. $S=\mathrm{PSL}_2(s)$ and $s\in\{5,7,9,11,13,17,19,23,25\}$,
2. $S=\mathrm{PSL}_3(3)$,
3. $S=\mathrm{PSp}_4(3)$ or $S=\mathrm{PSp}_4(5)$,
4. $S=\mathrm{PSU}_3(3)$ or $S=\mathrm{PSU}_4(3)$.

In these cases the maximum element order in $\mathrm{Aut}(S)$ is at most 30 by the ATLAS [9]. But the image of the linear Singer cycle in $\overline{X}$ has order 63, and so cannot be contained in $\mathrm{Aut}(S)$.

So $X=\mathrm{GU}_{2n}(q)$. In this case we have a 6-degree projective representation in characteristic 2. Thus s is odd and $e(S)\leqslant 6$. Again examining the possible values of $e(S)$ in Table 6.2, the only cases where we get integer solutions to this inequality are when

1. $S = \mathrm{PSL}_2(s)$ and $s \in \{5, 7, 9, 11, 13\}$,

2. $S = \mathrm{PSp}_4(3)$,

3. $S = \mathrm{PSU}_3(3)$ or $S = \mathrm{PSU}_4(3)$.

We can rule out all cases except $S = \mathrm{PSU}_4(3)$, by the previous argument as the image of the linear Singer cycle in $\overline{X}$ has order 21 and the maximum element order in $\mathrm{Aut}(S)$ is at most 14. But if $S = \mathrm{PSU}_4(3)$, then by the ATLAS [9, p. 52], $\mathrm{Aut}(S)$ contains no element of order 21.

Therefore this means $(n, q) \neq (6/u, 2)$ and so $X = \mathrm{Sp}_{2n}(q)$ and $n = 2$. Thus S has a 4-degree projective representation and $e(S) \leqslant 4$. Once again examining the possible values of $e(S)$ in Table 6.2, we only get integer solutions to this inequality when

1. $S = \mathrm{PSL}_2(s)$ and $s \in \{4, 5, 7, 9\}$,

2. $S = \mathrm{PSL}_3(2)$ or $S = \mathrm{PSL}_3(4)$,

3. $S = \mathrm{PSp}_4(2)$ or $S = \mathrm{PSp}_4(3)$,

4. $S = \mathrm{PSU}_4(2)$.

Using the known isomorphisms of some of these classical groups and noting that we have already considered the case when S is an alternating group, we only need to consider when S is one of $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_3(4)$ or $\mathrm{PSp}_4(3)$. If $S = \mathrm{PSL}_2(7)$, then the maximum element order in $\mathrm{Aut}(\mathrm{PSL}_2(7))$ is 8 and Inequality 6.1.1 gives $q = 2$ or 3. However 7 divides the order of S, but not the order of $\mathrm{PSp}_4(q)$, for these values of q.

If $S = \mathrm{PSL}_3(4)$, then the maximum element order in $\mathrm{Aut}(\mathrm{PSL}_3(4))$ is 21 and Inequality 6.1.1 gives $q = 2$, 3, 4 or 5. But again, for these values of q, 7 divides the order of S, but not the order of $\mathrm{PSp}_4(q)$.

Finally if $S = \mathrm{PSp}_4(3)$, then the maximum element order in $\mathrm{Aut}(\mathrm{PSp}_4(3))$ is 12. This time Inequality 6.1.1 gives $q = 2$, 3 or 5. Since q is coprime to s, we can ignore $q = 3$, so in fact $q = 2$ or 5. But 81 divides the order of S but not the order of $\mathrm{PSp}_4(q)$ for these values of q.

This contradiction concludes the proof of the proposition. $\square$

We can now assume that $q^{un} - 1$ has a primitive prime divisor. As already mentioned, we use a similar method to [15, Proposition 8.1]. A result of Hering gives an upper bound, $r_{\max}$ for the largest prime dividing the order of S. Also by looking at the values of $|\mathrm{Out}(S)|$ given in [24, Page 170], we note that $r_{\max} \geqslant |\mathrm{Out}(S)|$, so these bounds also hold for $|\mathrm{Aut}(S)|$. Therefore by Remark 2.2.3, we have

$$un \leqslant r - 1 \leqslant r_{\max} - 1.$$

Also our simple group, S has a projective representation of degree $2n$ and so the Landazuri-Seitz bounds give

$$e(S) \leqslant 2n. \tag{6.3.1}$$

Putting these together give

$$u \cdot e(S)/2 \leqslant un \leqslant r_{\max} - 1. \tag{6.3.2}$$

In most of the cases for S, this gives a contradiction. These cases are given in Table 6.3.

We still have to consider a few finite cases for small values of s. These are when S is $\mathrm{PSp}_4(4)$, $\mathrm{PSp}_6(2)$, $\mathrm{PSU}_4(3)$, $\mathrm{P}\Omega_8^{\pm}(2)$, $\mathrm{G}_2(3)$, $\mathrm{G}_2(4)$, ${}^3\mathrm{D}_4(2)$, ${}^2\mathrm{F}_4(2)'$ or ${}^2\mathrm{B}_2(8)$, when $X = \mathrm{Sp}_{2n}(q)$ or $\mathrm{GO}_{2n}^{+}(q)$ and $\mathrm{G}_2(4)$, ${}^2\mathrm{F}_4(2)'$ or ${}^2\mathrm{B}_2(8)$, when $X = \mathrm{GU}_{2n}(q)$. We also need to consider three infinite cases. These are when S is $\mathrm{PSp}_{2k}(s)$, for s odd; $\mathrm{PSU}_k(s)$, for k odd; or $\mathrm{PSL}_k(s)$.

We first deal with the finite cases.

Proposition 6.3.3 *Suppose that $n \geqslant 4 - u$ and $(n, q) \neq (6/u, 2)$ and let G be a subgroup*

S	$e(S)$	$r_{\max}$	conditions
$\mathrm{Sp}_{2k}(s)$	$\frac{1}{2}s^{k-1}\left(s^{k-1}-1\right)(s-1)$	s^k+1	$k \geqslant 2$, s even, $(k,s) \neq (2,2), (3,2)$
$\mathrm{PSU}_k(s)$	$\frac{s^k-1}{s+1}$ $\frac{s^4-1}{s+1}$	$\frac{s^{k-1}+1}{s+1}$ s^2+1	$k \geqslant 6$, k even, $k=4$, $s \neq 2, 3$
$\mathrm{P}\Omega^+_{2k}(s)$	$\left(s^{k-1}-1\right)\left(s^{k-2}+1\right)$ $s^{k-2}\left(s^{k-1}-1\right)$	$\frac{s^k-1}{s-1}$ $\frac{s^k+1}{\gcd\left(4,s^k-1\right)}$	$k \geqslant 4$, $s \neq 2, 3, 5$ $k \geqslant 4$, $s = 2, 3, 5$, $(k,s) \neq (4,2)$
$\mathrm{P}\Omega^-_{2k}(s)$	$\left(s^{k-1}+1\right)\left(s^{k-2}-1\right)$	$\frac{s^k+1}{\gcd\left(4,s^k-1\right)}$	$k \geqslant 4$, $(k,s) \neq (4,2)$
$\Omega_{2k+1}(s)$	$s^{2(k-1)}-1$ $s^{k-1}\left(s^{k-1}-1\right)$ 27	$\frac{1}{2}\left(s^k+1\right)$ $\frac{1}{2}\left(s^k+1\right)$ 13	$k \geqslant 3$, $s > 5$ $s=5$ or $s=3$ and $k>3$ $s=k=3$
$\mathrm{E}_6(s)$	$s^9\left(s^2-1\right)$	s^6+s^3+1	
$\mathrm{E}_7(s)$	$s^{15}\left(s^2-1\right)$	$\frac{s^7-1}{s-1}$	
$\mathrm{E}_8(s)$	$s^{27}\left(s^2-1\right)$	$s^8+s^7-s^5-s^4$ $-s^3+s+1$	
$\mathrm{F}_4(s)$	$s^6\left(s^2-1\right)$ $\frac{1}{2}s^7\left(s^3-1\right)(s-1)$ 44	s^4+1 s^4+1 17	s odd s even, $s \geqslant 4$ $s=2$
${}^2\mathrm{E}_6(s)$	$s^9\left(s^2-1\right)$	s^6-s^3+1	
$\mathrm{G}_2(s)$	$s\left(s^2-1\right)$	s^2+s+1	$s \geqslant 5$
${}^3\mathrm{D}_4(s)$	$s^3\left(s^2-1\right)$	s^4-s^2+1	$s \geqslant 3$
${}^2\mathrm{F}_4(s)$	$s^4(s-1)\left(\frac{1}{2}s\right)^{1/2}$	s^4-s^2+1	$s=2^{2m+1}>2$
${}^2\mathrm{B}_2(s)$	$(s-1)\left(\frac{1}{2}s\right)^{1/2}$	$s+(2s)^{1/2}+1$	$s=2^{2m+1}>8$
${}^2\mathrm{G}_2(s)$	$s(s-1)$	$s+(3s)^{1/2}+1$	$s=3^{2m+1} \geqslant 27$

Table 6.3: Values of $e(S)$ and $r_{\max}$ that contradict Inequality 6.3.2.

S	meo (Aut (S))	$e(S)$	S	meo (Aut (S))	$e(S)$
$\mathrm{PSp}_4(4)$	20	18	$\mathrm{G}_2(3)$	18	14
$\mathrm{PSp}_6(2)$	15	7	$\mathrm{G}_2(4)$	24	12
$\mathrm{PSU}_4(3)$	28	6	${}^3\mathrm{D}_4(2)$	28	24
$\mathrm{P}\Omega_8^+(2)$	30	8	${}^2\mathrm{F}_4(2)'$	20	26
$\mathrm{P}\Omega_8^-(2)$	30	27	${}^2\mathrm{B}_2(8)$	15	8

Table 6.4: meo (Aut (S)) and $e(S)$, for the finite cases.

of X. Also, suppose G lies in $\mathcal{S}$ and the socle, S of $G/\mathrm{Z}(X)$ is one of the groups in Table 6.4. Also, assume that q is not divisible by 3, when $S = \mathrm{G}_2(3)$ or $\mathrm{PSU}_4(3)$ and q is odd in the other cases. Then G does not contain a linear Singer cycle of X.

Proof. Table 6.4 gives the possibilities for S as well as the maximum element order in their automorphism groups which we have taken from the ATLAS [9]. We have also given a lower bound on the minimum degree of a projective representation of S in non defining characteristic, which we have taken from [24, p. 188].

Suppose that G contains a linear Singer cycle of X. If $X = \mathrm{GU}_{2n}(q)$, then $S = \mathrm{G}_2(4)$, ${}^2\mathrm{F}_4(2)'$ or ${}^2\mathrm{B}_2(8)$. But using Inequality 6.1.1 together with Inequality 6.3.1 gives a contradiction.

Hence $X \neq \mathrm{GU}_{2n}(q)$ and S is one of the groups in Table 6.4. We can again use Inequality 6.1.1 and Inequality 6.3.1 to rule out all but a few cases. These are $S = \mathrm{PSp}_6(2)$, $\mathrm{P}\Omega_8^+(2)$ or ${}^2\mathrm{B}_2(8)$, when $(n,q) = (4,2)$ and $S = \mathrm{PSU}_4(3)$, when $(n,q) = (3,2)$, $(3,3)$ or $(4,2)$. By our assumptions on q, we only need to consider $S = \mathrm{PSU}_4(3)$ and $(n,q) = (3,2)$ or $(4,2)$. But for these values of n and q, we observe that 729 divides the order of S but not the order of $\overline{X}$, so $\mathrm{PSU}_4(3)$ cannot embed in $\overline{X}$.

Since we have exhausted the possibilities for S, this gives the required result. □

The following three propositions deal with the infinite cases.

Proposition 6.3.4 *Suppose that $n \geqslant 4-u$ and $(n,q) \neq (6/u,2)$ and let G be a subgroup of X lying in $\mathcal{S}$. Also, suppose that the socle S of G is $\mathrm{PSL}_k(s)$ and assume that s and q are coprime. If G contains a linear Singer cycle of X, then $X = \mathrm{Sp}_6(3)$ and G is conjugate to one of two copies of $\mathrm{SL}_2(13)$.*

Proof. We distinguish between the cases when $k=2$ and when $k \geqslant 3$. Suppose first that $k=2$. We do not need to consider $S = \mathrm{PSL}_2(4)$ or $\mathrm{PSL}_2(9)$ as these were dealt with in the alternating groups case. Therefore using the Landazuri-Seitz bounds, Inequality 6.3.1 gives

$$(s-1)\,/\,\mathrm{gcd}\,(2, s-1) \leqslant 2n.$$

Also, by Theorem 2.2.6, the largest element order in $\mathrm{Aut}\,(S)$ is $s+1$. Therefore, since G contains a linear Singer cycle of X, we have

$$(q^{un}-1)\,/d \leqslant s+1 \leqslant 2n\,\mathrm{gcd}\,(2, s-1)+1+1 \leqslant 4n+2. \tag{6.3.3}$$

If $X = \mathrm{GU}_{2n}(q)$, then the only integer solution to this inequality with $n \geqslant 2$ and q a power of a prime is $(n,q) = (2,2)$. For this value of n, Inequality 6.3.1 gives $s = 4, 5, 7$ or 9. Since the alternating groups have already been dealt with, we only need to consider $S = \mathrm{PSL}_2(7)$. Now, $\mathrm{Aut}\,(\mathrm{PSL}_2(7)) = \mathrm{PGL}_2(7)$ and the image of the linear Singer cycle of X in $\mathrm{PGU}_4(2)$ has order 5. But 5 does not divide the order of $\mathrm{PGL}_2(7)$.

Hence $X \neq \mathrm{GU}_{2n}(q)$. In this case, the only integer solutions to Inequality 6.3.3 with $n \geqslant 3$ and q a power of a prime are $(n,q) = (3,2), (3,3)$ and $(4,2)$. With these values of n, we again use Inequality 6.3.1 to determine the values of s. Ignoring any values of s that are not copime to q and values such that S is an alternating group, we get

1. $s = 7, 11$ or 13, when $n = 3$;

2. $s = 7, 11, 13$ or 17, when $n = 4$.

When $n = 4$, the image of the linear Singer cycle in $\overline{X}$ has order 15. However by the ATLAS [9, p. 3, 7-9], for these values of s, $\mathrm{Aut}\,(S) = \mathrm{PGL}_2\,(s)$ contains no element of such order.

So $n = 3$. The image of the linear Singer cycle in $\overline{X}$ has order 7 or 13, when $q = 2$ or 3, respectively. Since the order of $\mathrm{Aut}\,(\mathrm{PSL}_2\,(11))$ is not divisible by 7 or 13, we can rule these cases out. If $s = 7$, then the order of $\mathrm{Aut}\,(S)$ is not divisible by 13, so we can immediately rule out the case when $q = 3$. If $q = 2$, then using MAGMA [5], we can see in $\mathrm{Sp}_6\,(2)$ and $\mathrm{GO}_6^+\,(2)$, there are two conjugacy classes of subgroups isomorphic to $\mathrm{PSL}_2\,(7)$, however these lie in $\mathcal{C}_1$ and are not irreducible. Therefore $s = 13$. If $q = 2$, then 13 divides the order of S, but not the order of $\overline{X}$, so this case is ruled out. Similarly, we can ignore the case when $\overline{X} = \mathrm{PGO}_6^+\,(3)$, as 7 divides the order of S but not the order of $\overline{X}$.

This leaves the case when $\overline{X} = \mathrm{PSp}_6\,(3)$. Here, there are two conjugacy classes of groups isomorphic to $\mathrm{PSL}_2\,(13)$ lying in $\mathcal{S}$, from MAGMA [5] and [6, Table 8.29]. In $\mathrm{Sp}_6\,(3)$, these correspond to conjugacy classes of groups isomorphic to $\mathrm{SL}_2\,(13)$. Moreover all subgroups of order 26 in $\mathrm{Sp}_6\,(3)$ are cyclic and conjugate. Therefore, since the order of a linear Singer cycle is 26, the linear Singer cycle is contained in a conjugate of one of these copies of $\mathrm{SL}_2\,(13)$. Since $G/\mathrm{Z}\,(X)$ is almost simple and the subgroups isomorphic to $\mathrm{SL}_2\,(13)$ are maximal subgroups of $\mathrm{Sp}_6\,(3)$, we conclude G is conjugate to one of these two copies of $\mathrm{SL}_2\,(13)$.

Therefore we can now assume that $k \geqslant 3$. We do not need to consider $S = \mathrm{PSL}_3\,(2)$ as this was dealt with when we considered $S = \mathrm{PSL}_2\,(7)$. If $S = \mathrm{PSL}_3\,(4)$, then the maximum element order in $\mathrm{Aut}\,(\mathrm{PSL}_3\,(4))$ is 21. If $X = \mathrm{GU}_{2n}\,(q)$, then the only integer solutions to Inequality 6.1.1 with $n \geqslant 2$, q a power of a prime and $(n, q) \neq (3, 2)$ are $(n, q) = (2, 2)$ and $(2, 3)$. We can immediately ignore $q = 2$, by our assumption on s. If $q = 3$ then the image of the linear Singer cycle in $\mathrm{PGU}_4\,(3)$ has order 20. But by the

ATLAS [9, P. 23], $\mathrm{Aut}(\mathrm{PSL}_3(4))$ has no elements of such order.

Hence $X \neq \mathrm{GU}_{2n}(q)$. This time the only integer solutions to Inequality 6.1.1 with $n \geqslant 3$, q a power of a prime and $(n, q) \neq (6, 2)$ are $(n, q) = (3, 2), (3, 3)$ and $(4, 2)$. We can again ignore both cases when $q = 2$, by our assumptions on s, so we only need to consider $(n, q) = (3, 3)$. But the image of the linear Singer cycle in $\overline{X}$ has order 13 which does not divide the order of $\mathrm{Aut}(\mathrm{PSL}_3(4))$.

Therefore $S \neq \mathrm{PSL}_3(2)$ or $\mathrm{PSL}_3(4)$ and so using the Landazuri-Seitz bounds, Inequality 6.3.1 gives

$$s^{k-1} - 1 \leqslant 2n.$$

Also, by Theorem 2.2.6, the largest element order in $\mathrm{Aut}(S)$ is $\left(s^k - 1\right)/(s-1)$. Therefore, since G contains a linear Singer cycle of X, we have

$$\begin{aligned} \left(q^{un} - 1\right)/d &\leqslant \left(s^k - 1\right)/(s-1) \\ &= s^{k-1} + s^{k-2} + \cdots + s + 1 \\ &= s^{k-1} + \left(s^{k-1} - 1\right)/(s-1) \\ &\leqslant s^{k-1} + s^{k-1} - 1 \\ &= 2\left(s^{k-1} - 1\right) + 1 \\ &\leqslant 4n + 1. \end{aligned} \tag{6.3.4}$$

If $X = \mathrm{GU}_{2n}(q)$, then the only integer solution to this inequality with $n \geqslant 2$ and q a power of a prime is $(n, q) = (2, 2)$. But for this value of n, Inequality 6.3.1 gives $(k, s) = (3, 2)$, which has already been dealt with.

So $X \neq \mathrm{GU}_{2n}(q)$, in which case the only integer solutions to Inequality 6.3.4 with $n \geqslant 3$ and q a power of a prime are $(n, q) = (3, 2), (3, 3)$ or $(4, 2)$. With these values of n, we again use Inequality 6.3.1 to determine the values of k and s. These are $(k, s) = (3, 2)$, when $n = 3$ and $(k, s) = (3, 2), (3, 3)$ or $(4, 2)$, when $n = 4$. Since $S \neq \mathrm{PSL}_3(2)$ and s is coprime to q, we only need to consider the case when $S = \mathrm{PSL}_3(3)$, when $(n, q) = (4, 2)$. In this case, the image of the linear Singer cycle in $\overline{X}$ has order 15. But 15 does not divide the order of $\mathrm{Aut}(\mathrm{PSL}_3(3))$.

This contradiction concludes the proof of the proposition. $\square$

Proposition 6.3.5 *Suppose $n \geqslant 4 - u$ and $(n, q) \neq (6/u, 2)$ and let G be a subgroup of X. Also suppose G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is $\mathrm{PSp}_{2k}(s)$, where s is coprime to q and s is odd. Then G does not contain a linear Singer cycle of X.*

Proof. Since s is odd and S has a $2n$-dimensional projective representation, Inequality 6.3.1 becomes

$$\left(s^k - 1\right)/2 \leqslant 2n,$$

by the Landazuri-Seitz bounds. We also know the largest element order in $\mathrm{Aut}(S)$ is at most $s^{k+1}/(s-1)$, by Theorem 2.2.6. Therefore, if G contains a linear Singer cycle of X, we have

$$\begin{aligned}
(q^{un} - 1)/d &\leqslant s^{k+1}/(s-1) \\
&= s^k \cdot s/(s-1) \\
&\leqslant (4n+1)(1 + 1/(s-1)) \\
&\leqslant 6n + 3/2. \qquad (6.3.5)
\end{aligned}$$

If $X = \mathrm{GU}_{2n}(q)$, then the only integer solution to this inequality with $n \geqslant 2$, q a power of a prime and $(n, q) \neq (3, 2)$ is $(n, q) = (2, 2)$. For this value of n, Inequality 6.3.1 then gives $(k, s) = (2, 3)$. But then

$$S = \mathrm{PSp}_4(3) \cong \mathrm{PGU}_4(2) = \overline{X}.$$

Therefore $X \neq \mathrm{GU}_{2n}(q)$ in which case, the only integer solutions of Inequality 6.3.5 with $n \geqslant 3$ and q a power of a prime are $(n, q) = (3, 2), (3, 3), (4, 2)$ or $(5, 2)$. For each of these values of n, Inequality 6.3.1 gives $(k, s) = (2, 3)$. This means we cannot have $q = 3$, by our assumptions and so $\mathrm{PSp}_4(3)$ has an absolutely irreducible projective representation in characteristic 2 having degree 6, 8 or 10. But this contradicts the result of Hiss and Malle [17]. □

Proposition 6.3.6 *Suppose $n \geqslant 4 - u$ and $(n, q) \neq (6/u, 2)$ and let G be a subgroup of X lying in $\mathcal{S}$. Also suppose that the socle S of G is $\mathrm{PSU}_k(s)$, where s is coprime to q and k is odd. If G contains a linear Singer cycle of X, then $X = \mathrm{Sp}_6(2)$ and*

$$\mathrm{PSU}_3(3) \leqslant G \leqslant \mathrm{PSU}_3(3) : 2.$$

Proof. First assume that $S = \mathrm{PSU}_5(2)$. By the Landazuri-Seitz bounds, a lower bound for the minimum degree of a projective representation in odd characteristic is 10, so $10 \leqslant 2n$. On the other hand the largest possible element order in $\mathrm{Aut}(S)$ is 24 and so $(q^{un} - 1)/d \leqslant 24$, which has no integer solutions with $n \geqslant 5$ and q a power of a prime.

Therefore assume $S \neq \mathrm{PSU}_5(2)$. Then since k is odd and S has a $2n$-dimensional projective representation, using the Landazuri-Seitz bounds, Inequality 6.3.1 becomes

$$2n \geqslant s\left(s^{k-1} - 1\right)/(s+1) \geqslant s\left(s^2 - 1\right)/(s+1) = s(s-1) \geqslant s.$$

Also by Theorem 2.2.6, the largest element order in $\mathrm{Aut}(S)$ is at most $s^{k-1} + s$. Therefore, since G contains a linear Singer cycle of X, we have

$$\begin{aligned}(q^{un} - 1)/d &\leqslant s^{k-1} + s \\ &\leqslant 2n(s+1)/s + 1 + s\end{aligned}$$

$$\begin{aligned} &= 2n(1+1/s)+1+s \\ &\leqslant 2n\cdot 3/2+1+2n \\ &= 5n+1. \end{aligned} \tag{6.3.6}$$

If $X = \mathrm{GU}_{2n}(q)$, then the only integer solution to this inequality with $n \geqslant 2$ and q a power of a prime is $(n, q) = (2, 2)$. But for this value of n, Inequality 6.3.1 gives $(k, s) = (3, 2)$, which contradicts the simplicity of S.

Hence $X \neq \mathrm{GU}_{2n}(q)$. Then the only integer solutions of Inequality 6.3.6 with $n \geqslant 3$ and q a power of a prime are $(n, q) = (3, 2), (3, 3)$ or $(4, 2)$. For these values of n, Inequality 6.3.1 gives $(k, s) = (2, 3), (3, 3)$ or $(5, 2)$. By our assumptions and the simplicity of S, we only need to consider $(k, s) = (3, 3)$ and $(n, q) = (3, 2)$ or $(4, 2)$. We can immediately rule out $(n, q) = (4, 2)$, as the image of the linear Singer cycle in $\overline{X}$ has order 15 and the largest element order in $\mathrm{Aut}(\mathrm{PSU}_3(3))$ is 12 by the ATLAS [9]. Hence $(n, q) = (3, 2)$. If $\overline{X} = \mathrm{PGO}_6^+(2)$, then we note that 27 divides the order of S but not the order of $\overline{X}$ so this cannot happen.

Hence $\overline{X} = \mathrm{PSp}_6(2) = X$. Now

$$\mathrm{Aut}(\mathrm{PSU}_3(3)) = \mathrm{PSU}_3(3) : 2 \cong \mathrm{G}_2(2)$$

and there is a single conjugacy class of subgroups lying in $\mathcal{S}$ isomorphic to $\mathrm{PSU}_3(3) : 2$ in X by [6, Table 8.29]. Moreover the linear Singer cycle of X has order 7 and all subgroups of order 7 in X are conjugate, being Sylow-7 subgroups. Therefore the linear Singer cycle of X is contained in a conjugate of $\mathrm{PSU}_3(3) : 2$. Since $G/\mathrm{Z}(X)$ is almost simple, we conclude

$$\mathrm{PSU}_3(3) \leqslant G \leqslant \mathrm{PSU}_3(3) : 2,$$

as required. □

This concludes the proof of Theorem 6.3.1.

6.4 Lie-type groups in defining characteristic

Finally, we can assume that S is a simple group of Lie-type defined over $\mathrm{GF}(s)$, where $s = p^b$. In this section, we will prove the following Theorem.

Theorem 6.4.1 *Let G be a subgroup of X containing a linear Singer cycle of X. Also suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is a simple group of Lie-type defined over a field of characteristic p. Then G does not contain a linear Singer cycle of X.*

As in the non-defining characteristic case, we use the same approach as [15, Proposition 7.2]. If G contains a linear Singer cycle of X, then since $G \in \mathcal{S}$, $\mathrm{Aut}(S)$ contains an element of order $(q^{un} - 1)/d$. This means the order of $\mathrm{Aut}(S)$ is divisible by a primitive prime divisor of $q^{un} - 1$, if one exists. We use this to determine an upper bound on n.

We also have lower bounds on the minimum degree of a projective representation of a Lie-type group in defining characteristic, which we use to obtain a lower bound on n. These values are given in Table 6.5 which we have taken from [24, Proposition 5.4.13]. Here $\mathrm{R}_p(S)$ denotes the minimum degree of a projective representation of S in characteristic p. We will also make use of results from [24, Section 5.4] and [26] in our analysis.

But first, as in the non-defining characteristic case, we need to deal with the case when $q^{un} - 1$ has no primitive prime divisors. Throughout the remainder of this thesis, let $q = p^a$.

Proposition 6.4.2 *Let G be a subgroup of X and suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is a simple group of Lie-type defined over a field whose characteristic divides q. If $q^{un} - 1$ does not have a primitive prime divisor, then G does not contain a linear Singer cycle of X.*

S	$\mathrm{R}_p(S)$
$\mathrm{PSL}_k(s)\,;\mathrm{PSU}_k(s)\,,k\geqslant 3$	k
$\mathrm{PSp}_{2k}(s)\,,k\geqslant 2;\mathrm{P}\Omega^{\pm}_{2k}(s)\,,k\geqslant 4$	$2k$
$\Omega_{2k+1}(s)\,,k\geqslant 3, s$ odd	$2k+1$
$\mathrm{E}_6(s)\,;{}^2\mathrm{E}_6(s)$	27
$\mathrm{E}_7(s)$	56
$\mathrm{E}_8(s)$	248
$\mathrm{F}_4(s)$	$26-\delta_{p,3}$
$\mathrm{G}_2(s)$	$7-\delta_{p,2}$
${}^3\mathrm{D}_4(s)$	8
${}^2\mathrm{F}_4(s)'\,,\ S=2^{2m+1}$	26
${}^2\mathrm{B}_2(s)\,,\ s=2^{2m+1}$	4
${}^2\mathrm{G}_2(s)\,,\ s=3^{2m+1}$	7

Table 6.5: Minimum degrees of projective representations in characteristic p of Lie-type groups, S defined over characteristic p.

Proof. Suppose that G contains a linear Singer cycle of X. Since a primitive prime divisor of $q^{un}-1$ does not exist, by Theorem 2.2.2 and our assumptions on n, we either have $(n,q)=(6/u,2)$ or $X=\mathrm{Sp}_{2n}(q)$ and $n=2$.

Suppose first that $(n,q)=(6/u,2)$ and assume that $X\neq \mathrm{GU}_{2n}(q)$. Then, we have a 12-degree projective representation over $\mathrm{GF}(2)$ and $\mathrm{R}_2(S)\leqslant 12$. By looking at the values of $\mathrm{R}_p(S)$ in Table 6.5, we only need to consider the cases when S is one of $\mathrm{PSL}_k(s)\,,\ \mathrm{PSU}_k(s)\,,\ \mathrm{PSp}_{2k}(s)\,,\ \mathrm{P}\Omega^{\pm}_{2k}(s)\,,\ \mathrm{G}_2(s)$, ${}^3\mathrm{D}_4(s)$ or ${}^2\mathrm{B}_2(s)$.

Note that in this case $a=1$. Therefore by [24, Proposition 5.4.6, Remark 5.4.7], we have

$$12\geqslant \mathrm{R}_2(S)^b\,. \tag{6.4.1}$$

If S is either ${}^2\mathrm{B}_2(s)$ or $\mathrm{G}_2(s)$, then Inequality 6.4.1 gives $b=1$ and so S is either ${}^2\mathrm{B}_2(2)$

or $G_2(2)$. But ${}^2B_2(2)$ is not simple and since $G_2(2)' \cong PSU_3(3)$, we do not need to consider this case.

Similarly, if $S = {}^3D_4(s)$, then from Inequality 6.4.1, we also get $b = 1$ and so $S = {}^3D_4(2)$. But the image of the linear Singer cycle in $\overline{X}$ has order 63, and it can be seen from the ATLAS [9, p. 89] that $\mathrm{Aut}({}^3D_4(2))$ contains no element of such order.

If $S = P\Omega^{\pm}_{2k}(s)$, then Inequality 6.4.1 gives $b = 1$ and $k = 4$, 5 or 6. By [26], $P\Omega^{\pm}_8(2)$ and $P\Omega^{\pm}_{10}(s)$ have no irreducible 12-degree projective representations, so $S = P\Omega^{\pm}_{12}(2)$. If $X = Sp_{12}(2)$, then S is contained in $\mathcal{C}_8$, so we can assume $X = GO^{+}_{12}(2)$. But if $S = P\Omega^{-}_{12}(2)$, then 13 divides the order of S but not the order of X and if $S = P\Omega^{+}_{12}(2)$, then this contradicts our assumptions on G.

If $S = PSp_{2k}(s)$, then from Inequality 6.4.1, we have $b = 1$ and $k = 2$, 3, 4, 5 or 6. We do not consider $k = 2$, since then $S = PSp_4(2)$ which was already considered in the alternating groups case. Also if $k = 3$, 4 or 5, then S does not have any irreducible 12-degree projective representations by [26], so we can also rule out these cases. Hence $S = PSp_{12}(2)$. But if $X = Sp_{12}(2)$, then G is not a proper subgroup of X and if $X = GO^{+}_{12}(2)$, then the order of S is larger than the order of X.

Lastly, if $S = PSL_k(s)$ or $PSU_k(s)$, then Inequality 6.4.1 and [24, Theorem 5.4.6], give $b = 1$ and $2 \leqslant k \leqslant 12$. Since S is simple and recalling $PSL_3(2) \cong PSL_2(7)$, $PSL_4(2) \cong A_8$ and $PSU_4(2) \cong PSp_4(3)$, we may assume $k \geqslant 5$. Also, by [26], we can ignore the cases when $5 \leqslant k \leqslant 11$ as for these values of k, S has no irreducible 12-degree representations. Therefore S is either $PSL_{12}(2)$ or $PSU_{12}(2)$. But the orders of these groups are much larger than the order of $\overline{X}$.

Hence we can assume $X = GU_{2n}(q)$. In this case we have a 6-degree projective representation over $GF(4)$ and $R_2(S) \leqslant 6$. Comparing the values of $R_p(S)$ in Table 6.5 as before, we only need to consider the cases when S is one of $PSL_k(s)$, $PSU_k(s)$, $PSp_{2k}(s)$, $G_2(s)$ or ${}^2B_2(s)$.

First assume $S \neq \mathrm{PSU}_k(s)$. Then by [24, Proposition 5.4.6, Remark 5.4.7] and since $a = 2$, we have $b = 2f$ for some positive integer f and

$$6 \geqslant \mathrm{R}_2(S)^f . \tag{6.4.2}$$

This immediately rules out $S = {}^2\mathrm{B}_2(s)$ as b is odd in this case.

If $S = \mathrm{G}_2(s)$, then by Inequality 6.4.2, we have $f = 1$ and so $b = 2$. This means $S = \mathrm{G}_2(4)$. But 13 divides the order of S, but not the order of $\mathrm{PGU}_6(2)$.

If $S = \mathrm{PSp}_{2k}(s)$, then Inequality 6.4.2 gives $f = 1$ and $k = 2$ or 3. But for these values of k, 17 divides the order of $\mathrm{PSp}_{2k}(4)$, but not the order of $\mathrm{PGU}_6(2)$.

If $S = \mathrm{PSL}_k(s)$, then by Inequality 6.4.2, we have $f = 1$ and $k = 2$, 3, 4, 5 or 6. We can ignore $k = 2$, since then $S = \mathrm{PSL}_2(4) \cong \mathrm{A}_5$, which has already been dealt with. Also, we can ignore $k = 4$, , 5 and 6 as for these values of k, 17 divides the order of $\mathrm{PSL}_k(4)$ but not the order of $\mathrm{PGU}_6(2)$. This leaves $S = \mathrm{PSL}_3(4)$. Now, there are two conjugacy classes of subgroups isomorphic to $\mathrm{PSL}_3(4)$ in $\mathrm{PGU}_6(2)$ by MAGMA [5] and the ATLAS [9, p. 115]. However none of these are irreducible.

Hence we can assume that $S = \mathrm{PSU}_k(s)$. By [24, Proposition 5.4.6], either $b = 2f$ or $b = f$ and b is odd, for some positive integer f. In the former case, we have $6 \geqslant k^f$ and so $f = 1$ and $k = 3$, 4, 5 or 6. But then $S = \mathrm{PSU}_k(4)$ and for these values of k, we note 13 divides the order of S, but not the order of $\mathrm{PGU}_6(2)$. Therefore $b = f$ and b is odd. As before, we have $f = 1$ and $k = 3$, 4, 5 or 6 and $S = \mathrm{PSU}_k(2)$. By the simplicity of S and since $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$, we can ignore $k = 3$ or 4. Also $\mathrm{PSU}_5(2)$ has no irreducible representations of degree 6 by [26], so this case is ruled out. Therefore $S = \mathrm{PSU}_6(2)$. But the image of the linear Singer cycle in $\mathrm{PGU}_6(2)$ has order 21 and $\mathrm{PSU}_6(2)$ contains no elements of such order.

Finally we can assume that $(n, q) \neq (6/u, 2)$, so $X = \mathrm{Sp}_{2n}(q)$ and $n = 2$. We have a 4-degree projective representation and $R_p(S) \leqslant 4$. We again compare the values of $R_p(S)$ in Table 6.5. This time we only need to consider the cases when S is one of $PSL_k(s)$, $PSU_k(s)$, $PSp_{2k}(s)$ or ${}^2B_2(s)$.

First consider the case when $S \neq PSU_k(s)$. Then by [24, Proposition 5.4.6, Remark 5.4.7], we have $b = af$ for some positive integer f and

$$4 \geqslant R_p(S)^f. \tag{6.4.3}$$

If $S = {}^2B_2(s)$, then Inequality 6.4.3 gives $f = 1$ and so $s = q = 2^{2m+1}$. By [14, Theorem 1.2, Table 4], the maximum element order in $\mathrm{Aut}({}^2B_2(q))$ is $(q^2+1)/4$ and so if $\mathrm{Aut}(S)$ contains a linear Singer cycle of $Sp_4(q)$, we have $q^2 - 1 \leqslant (q^2+1)/4$, which cannot happen.

If $S = PSp_{2k}(s)$, then by Inequality 6.4.3, we have $f = 1$ and $k = 2$. But then $S = PSp_4(q)$, so G is not a proper subgroup of $Sp_4(q)$.

If $S = PSL_k(s)$, by Inequality 6.4.3, we have $(f,k) = (1,2), (1,3), (1,4)$ or $(2,2)$. We can immediately ignore $(f,k) = (1,4)$, as then the order of S is larger than the order of $PSp_4(q)$. We can also ignore the case when $(f,k) = (1,3)$, as $PSL_3(q)$ has no irreducible 4-degree representations by [26]. Also by [6, Theorem 5.3.9], there are no subgroups of $PSp_4(q)$ isomorphic to $PSL_2(q^2)$ lying in $\mathcal{S}$, so we also rule out $(f,k) = (2,2)$. Now if $(f,k) = (1,2)$, then $S = PSL_2(q)$. Since we have already dealt with the alternating groups, $q \neq 4$ and so the maximum element order in $\mathrm{Aut}(PSL_2(q))$ is $q+1$, by Theorem 2.2.6. Therefore since G contains a linear Singer cycle of $Sp_4(q)$, we have

$$\left(q^2 - 1\right) / \gcd(2, q-1) \leqslant q + 1,$$

which gives $q = 2$ or 3. This contradicts the simplicity of S.

So we can assume that $S = PSU_k(s)$. By [24, Proposition 5.4.6], either $b = af$ or

$2b = af$ and a does not divide b, for some positive integer f. In both cases we have $\mathrm{R}_p(S)^f \leqslant 4$, which gives $f = 1$ and $k = 3$ or 4. We can immediately rule out $k = 3$, because $\mathrm{PSU}_3(s)$ has no irreducible 4-degree prepresentations by [26]. If $b = af$, then $S = \mathrm{PSU}_4(q)$ lying in $\mathrm{PSp}_4(q)$. But the order of $\mathrm{PSU}_4(q)$ is larger than the order of $\mathrm{PSp}_4(q)$. Therefore $2b = af$, where a does not divide b and $S = \mathrm{PSU}_4(s)$ lying in $\mathrm{PSp}_4(s^2)$. Now $s \neq 2$, since then $S = \mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$, which has already been dealt with. Therefore $s^6 - 1$ has a primitive prime divisor, r. But we can observe that r divides the order of $\mathrm{PSU}_4(s)$, but not the order of $\mathrm{PSp}_4(s^2)$.

This contradiction concludes the proof of the proposition. □

Therefore, we can now assume $q^{un} - 1$ has a primitive prime divisor, r. Suppose further that r divides $|\mathrm{Out}(S)|$ but not the order of S. Arguing exactly as in [15, Proposition 7.2] and by expecting the orders of $|\mathrm{Out}(S)|$ in [24, p. 170], we see that r divides a. Also r divides the order of G, so G contains an element of order r, which must be a field automorphism in $\mathrm{Out}(S)$. This automorphism preserves our irreducible $2n$-dimensional G-module. Hence by [24, 5.4.2, 5.4.5], we have $2n \geqslant 2^r$. Hence by Remark 2.2.3, we have

$$r - 1 \geqslant un \geqslant n \geqslant 2^{r-1},$$

which is a contradiction.

Therefore we can assume that r divides $|S|$. By inspecting the orders of S in [24, p. 170] and noting, if r divides $s^8 + s^4 + 1$, then r divides

$$\left(s^8 + s^4 + 1\right)\left(s^4 - 1\right) = s^{12} - 1,$$

we observe that r divides $s^x - 1 = p^{xb} - 1$. But by [24, 5.4.6, 5.4.7], we can write $b = af/c$, where $c = 1$, 2 or 3 depending on S. Therefore r divides $p^{axf/c} - 1 = q^{xf/c} - 1$. By Remark 2.2.3, this means that un divides xf/c. This also gives an upper bound on un.

The values we take for x are given in Table 6.6. They can easily be found by inspecting the order of S.

S	x
$\mathrm{PSL}_k(s)$;	k
$\mathrm{PSp}_{2k}(s)$, $k \geqslant 2$; $\mathrm{PSU}_k(s)$, $k \geqslant 3$; $\mathrm{P\Omega}^-_{2k}(s)$, $k \geqslant 4$; $\Omega_{2k+1}(s)$, $k \geqslant 3$	$2k$
$\mathrm{P\Omega}^+_{2k}(s), k \geqslant 4,$	$2k-2$
$\mathrm{E}_6(s)$; ${}^3\mathrm{D}_4(s)$, $\mathrm{F}_4(s)$, ${}^2\mathrm{F}_4(s)'$	12
$\mathrm{E}_7(s)$, ${}^2\mathrm{E}_6(s)$	18
$\mathrm{E}_8(s)$	30
$\mathrm{G}_2(s)$, ${}^2\mathrm{G}_2(s)$	6
${}^2\mathrm{B}_2(s)$, $s = 2^{2m+1}$	4

Table 6.6: Values for x

We also have a $2n$-dimensional projective representation of S and by [24, 5.4.6, 5.4.7], there is an irreducible module M such that $2n = \dim(M)^f$, so $\mathrm{R}_p(S)^f/2$ gives a lower bound on n.

If S is not $\mathrm{PSU}_k(s), \mathrm{P\Omega}^-_{2k}(s), {}^2\mathrm{E}_6(s)$ or ${}^3\mathrm{D}_4(s)$, then by [24, 5.4.6, 5.4.7] and Table 6.5, we have $b = af$ and

$$xf \geqslant n \geqslant \mathrm{R}_p(S)^f/2. \tag{6.4.4}$$

If S is $\mathrm{PSU}_k(s)$, $\mathrm{P\Omega}^-_{2k}(s)$,or ${}^2\mathrm{E}_6(s)$, then by [24, 5.4.6, 5.4.7] and Table 6.5, we either have $b = af$ and Inequalities 6.4.4 hold, or $2b = af$, where a does not divide b and we have

$$xf/2 \geqslant n \geqslant \mathrm{R}_p(S)^f/2. \tag{6.4.5}$$

If S is ${}^3\mathrm{D}_4(s)$, then by [24, 5.4.7] and Table 6.5, we either have $b = af$ and Inequalities 6.4.4 hold, or $3b = af$, where a does not divide b and we have

$$xf/3 \geqslant n \geqslant \mathrm{R}_p(S)^f/2. \qquad (6.4.6)$$

These bounds enable us to rule out a lot of cases for n. If $f = 1$ though, we shall need to use [24, 5.4.11] to determine the values of n.

We begin with the situation when S is not $\mathrm{PSU}_k(s), \mathrm{P}\Omega^-_{2k}(s), {}^2\mathrm{E}_6(s)$ or ${}^3\mathrm{D}_4(s)$.

Proposition 6.4.3 *Suppose $n \geqslant 4-u$ and $(n,q) \neq (6/u,2)$ and let G be a subgroup of X. Suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is a simple group of Lie-type other than $\mathrm{PSU}_k(s)$, $\mathrm{P}\Omega^-_{2k}(s)$, ${}^2\mathrm{E}_6(s)$ or ${}^3\mathrm{D}_4(s)$, where $s = p^b$. Then G does not contain a linear Singer cycle of X.*

Proof. By [24, Proposition 5.4.6, Remark 5.4.7], we have $b = af$, for some positive integer f and Inequality 6.4.4 holds. First assume that S is an exceptional group of Lie-type. Using the values in Table 6.5 and Table 6.6 in Inequality 6.4.4, we get a contradiction, unless $S = {}^2\mathrm{B}_2(s)$, ${}^2\mathrm{G}_2(s)$ or $\mathrm{G}_2(s)$.

If $S = {}^2\mathrm{B}_2(s)$, then Inequality 6.4.4 becomes

$$4f \geqslant un \geqslant 4^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we have $4f \geqslant 4^f$, which means $f = 1$ and $2n = 4$. We therefore have a possible embedding of ${}^2\mathrm{B}_2(q)$ in $\mathrm{PGU}_4(q)$. By [14, Theorem 1.2, Table 4], an upper bound for the element order of $\mathrm{Aut}({}^2\mathrm{B}_2(q))$ is $(q^2+1)/4$. Since G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, we have

$$\left(q^4-1\right)/(q+1) \leqslant \left(q^2+1\right)/4,$$

which has no solutions for q an odd power of 2.

Hence $X \neq \mathrm{GU}_{2n}(q)$, so we have $4f \geqslant 4^f/2$. Since b is odd, this gives $f = 1$. Also, n divides 4 and since $n \geqslant 3$, we get $2n = 8$. But this cannot happen by [26].

If $S = {}^2\mathrm{G}_2(s)$, then we have

$$6f \geqslant un \geqslant 7^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we get $6f \geqslant 7^f$, which cannot happen. So $X \neq \mathrm{GU}_{2n}(q)$, then we get $6f \geqslant 7^f/2$, which gives $f = 1$. Hence n divides 6 and $n \geqslant 7/2$. This means $2n = 12$. But by [26], this cannot happen.

If $S = \mathrm{G}_2(s)$, then Inequality 6.4.4 becomes

$$6f \geqslant un \geqslant (7 - \delta_{p,2})^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we have $6f \geqslant (7 - \delta_{p,2})^f$, and so $(f, p) = (1, 2)$ and $2n = 6$. We therefore have a possible embedding of $\mathrm{G}_2(q)$ in $\mathrm{PGU}_6(q)$. By the ATLAS [9, p. 97] and [14, Theorem 1.2, Table 4], an upper bound for the element order in $\mathrm{Aut}(\mathrm{G}_2(q))$ is 24, when $q = 4$ and $(q^6 - 1)/4(q - 1)$, when $q \geqslant 8$. But since G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, we have

$$\left(q^6 - 1\right)/(q+1) \leqslant \begin{cases} (q^6 - 1)/4(q - 1), & q \geqslant 8, \\ 24, & q = 4, \end{cases}$$

which has no solutions for q a power of 2.

So $X \neq \mathrm{GU}_{2n}(q)$. We have $6f \geqslant (7 - \delta_{p,2})^f/2$, and so $f = 1$. This means n divides 6 and since $n \geqslant (7 - \delta_{p,2})/2$, we either have $n = 6$ or $(n, p) = (3, 2)$. The former case is ruled out by [26], so we have a possible embedding of $\mathrm{G}_2(q)$ in $\mathrm{PSp}_6(q)$ or $\mathrm{PGO}_6^+(q)$

Now $q \neq 2$ so $q^6 - 1$ has a primitive prime divisor and we can observe that this prime divisor divides the order of $\mathrm{G}_2(q)$ but not the order of $\mathrm{PGO}_6^+(q)$, so $\mathrm{G}_2(q)$ does not embed in $\mathrm{PGO}_6^+(q)$. On the other hand $\mathrm{G}_2(q)$ is a maximal subgroup of $\mathrm{PSp}_6(q)$ by [6, Table 8.29]. By [28, Table 2], an upper bound for the element order $\mathrm{G}_2(q)$ is 21, when $q = 4$ and $8(q+1)^2$, when $q \geqslant 8$. If G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$, we have

$$q^3 - 1 \leqslant \begin{cases} 8(q+1)^2, & q \geqslant 8, \\ 21, & q = 4, \end{cases}$$

which gives $q = 8$. Examining the orders of the maximal subgroups of $\mathrm{G}_2(8)$ in [6, Table 8.30], the only maximal subgroup of $\mathrm{G}_2(8)$ whose order is divisible by $8^3 - 1 = 511$ is $\mathrm{SL}_3(8).2$. Thus if $\mathrm{G}_2(8)$ contains a linear Singer cycle of $\mathrm{Sp}_6(8)$, then so does $\mathrm{SL}_3(8).2$ But the largest possible element order in $\mathrm{SL}_3(8).2$ is at most $73 \cdot 2 = 146$, a contradiction.

Now we can assume that S is a classical group of Lie-type. If $S = \Omega_{2k+1}(s)$, then from Inequality 6.4.4, we have

$$2kf \geqslant un \geqslant (2k+1)^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we get $2kf \geqslant (2k+1)^f$, which cannot happen. So $X \neq \mathrm{GU}_{2n}(q)$ and $2kf \geqslant (2k+1)^f/2$, which implies $f = 1$. Hence n divides $2k$ and so since $n \geqslant (2k+1)/2$, we have $n = 2k$. We therefore have a possible embedding of $\Omega_{n+1}(q)$ in $\mathrm{PSp}_{2n}(q)$ or $\mathrm{PGO}_{2n}^+(q)$. By Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}(\Omega_{n+1}(q))$ is $q^{(n+2)/2}/(q-1)$. But if G contains a linear Singer cycle of X, we have

$$(q^n - 1)/2 \leqslant q^{(n+2)/2}/(q-1),$$

which has no integer solutions for $n \geqslant 6$ and q a power of an odd prime.

If $S = \mathrm{P}\Omega^{+}_{2k}(s)$ then Inequality 6.4.4 becomes,

$$2(k-1)f \geqslant un \geqslant (2k)^{f} u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then $2(k-1)f \geqslant (2k)^{f}$, which cannot happen. So $X \neq \mathrm{GU}_{2n}(q)$ and we get $2kf \geqslant (2k+1)^{f}/2$, which implies $f = 1$. Hence n divides $2(k-1)$ and since $n \geqslant k$, we have $n = 2(k-1)$. We therefore have a possible embedding of $\mathrm{P}\Omega^{+}_{n+2}(q)$ in $\mathrm{PSp}_{2n}(q)$ or $\mathrm{PGO}^{+}_{2n}(q)$. By Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}\left(\mathrm{P}\Omega^{+}_{n+2}(q)\right)$ is $q^{(n+4)/2}/(q-1)$. But if G contains a linear Singer cycle of X, we get

$$(q^{n}-1)/\gcd(2,q-1) \leqslant q^{(n+4)/2}/(q-1),$$

which has no integer solutions for $n \geqslant 6$ and q a power of a prime.

If $S = \mathrm{PSp}_{2k}(s)$, then Inequality 6.4.4 becomes

$$2kf \geqslant un \geqslant (2k)^{f} u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then $2kf \geqslant (2k)^{f}$, so $f = 1$ and $n = k$. We therefore have an embedding of $\mathrm{PSp}_{2n}(q)$ in $\mathrm{PGU}_{2n}(q)$. By Theorem 2.2.6, an upper bound for the element order of $\mathrm{Aut}(\mathrm{PSp}_{2n}(q))$ is $q^{n+1}/(q-1)$, so if G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, we have

$$\left(q^{2n}-1\right)/(q+1) \leqslant q^{n+1}/(q-1).$$

But this gives $(n,q) = (2,2)$ and so $S = \mathrm{PSp}_{4}(2) \cong \mathrm{S}_{6}$, which has already been dealt with.

Hence $X \neq \mathrm{GU}_{2n}(q)$ and we have $2kf \geqslant (2k)^{f}/2$. Hence $f = 1$ or $(f,k) = (2,2)$. In the latter case, we have $n = 8$ and we have a possible embedding of $\mathrm{PSp}_{4}(q^{2})$ in $\mathrm{PSp}_{16}(q)$

or $\mathrm{PGO}_{16}^{+}(q)$. By Theorem 2.2.6, an upper bound on the element order in $\mathrm{Aut}(\mathrm{PSp}_4(q^2))$ is $q^6/(q^2-1)$. But if G contains a linear Singer cycle of X, then

$$\left(q^8-1\right)/\gcd(2,q-1) \leqslant q^6/\left(q^2-1\right),$$

which has no integer solutions for q a power of a prime.

Hence $f=1$. Then n divides $2k$ and since $n \geqslant k$, we either have $n=2k$ or $n=k$. If $n=k$, then $S=\mathrm{PSp}_{2n}(q)$. Note that the order of $\mathrm{PSp}_{2n}(q)$ is larger than the order of $\mathrm{PGO}_{2n}^{+}(q)$, so we must have $X=\mathrm{Sp}_{2n}(q)$. But then G is not a proper subgroup of X.

So $n=2k$ and we have a possible embedding of $\mathrm{PSp}_n(q)$ in $\mathrm{PSp}_{2n}(q)$ or $\mathrm{PGO}_{2n}^{+}(q)$. By Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}(\mathrm{PSp}_n(q))$ is $q^{(n+2)/2}/(q-1)$. But if G contains a linear Singer cycle of X, then

$$(q^n-1)/\gcd(2,q-1) \leqslant q^{(n+2)/2}/(q-1),$$

which has no integer solutions for $n \geqslant 3$ and q a power of a prime.

Finally, suppose that $S=\mathrm{PSL}_k(s)$. Then Inequality 6.4.4 gives

$$kf \geqslant un \geqslant k^f u/2.$$

If $X=\mathrm{GU}_{2n}(q)$, then $kf \geqslant k^f$, so either $f=1$ or $(f,k)=(2,2)$. If $f=1$, then $2n=k$, so we have a possible embedding of $\mathrm{PSL}_{2n}(q)$ in $\mathrm{PGU}_{2n}(q)$. However this cannot happen because, if r is a primitive prime divisor of $q^{2n-1}-1$, then r divides the order of $\mathrm{PSL}_{2n}(q)$, but not the order of $\mathrm{PGU}_{2n}(q)$.

So $(f,k)=(2,2)$ and so $2n=4$. Thus we have a possible embedding of $\mathrm{PSL}_2(q^2)$ in $\mathrm{PGU}_4(q)$. Now $q \neq 2$, as then $S \cong \mathrm{A}_5$, so by Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}(\mathrm{PSL}_2(q^2))$ is q^2+1. But if G contains a linear Singer cycle of

$\mathrm{GU}_4(q)$, then we have

$$\left(q^4-1\right)/\left(q+1\right) \leqslant q^2+1,$$

which gives $q=2$, a contradiction.

Therefore $X \neq \mathrm{GU}_{2n}(q)$ and we get $kf \geqslant k^f/2$, so $1 \leqslant f \leqslant 4$. If $f=4$, then $k=2$ and $2n=16$. We therefore have a possible embedding of $\mathrm{PSL}_2(q^4)$ in $\mathrm{PSp}_{16}(q)$ or $\mathrm{PGO}^+_{16}(q)$. By Theorem 2.2.6 an upper bound on the element order of $\mathrm{Aut}(\mathrm{PSL}_2(q^4))$ is q^4+1. But if G contains a linear Singer cycle of X, we have

$$\left(q^8-1\right)/\gcd\left(2,q-1\right) \leqslant q^4+1,$$

which has no solutions for q a power of a prime.

If $f=3$, then $k=2$. Thus n divides 6 and so since $n \geqslant 4$, we have $2n=12$. But this cannot happen as $2n$ is a 3rd power by [24, Proposition 5.4.6].

If $f=2$, then $k=2$, 3 or 4. If $k=2$, then n divides 4, so since $n \geqslant 3$, we have $2n=8$ which is not a square. So by [24, Proposition 5.4.6], this cannot happen. Similarly, if $k=3$, then n divides 6 and since $n \geqslant 9/2$, we get $2n=12$, which also cannot happen by [24, Proposition 5.4.6]. If $k=4$ and $2n=16$. We therefore get a possible embedding of $\mathrm{PSL}_4(q^2)$ in $\mathrm{PSp}_{16}(q)$ or $\mathrm{PGO}^+_{16}(q)$. By Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}(\mathrm{PSL}_4(q^2))$ is $(q^8-1)/(q^2-1)$. But if G contains a linear Singer cycle of X, we get

$$\left(q^8-1\right)/\gcd\left(2,q-1\right) \leqslant \left(q^8-1\right)/\left(q^2-1\right),$$

which has no integer solutions for q a power of a prime.

Therefore we can assume $f=1$. If $2n=k$, then $S=\mathrm{PSL}_{2n}(q)$, which has a larger order than the order of $\overline{X}$. Hence, since $k \geqslant n \geqslant 3$, we have $2n \leqslant k(k+1)/2$ and so by [24, Proposition 5.4.11], $(k,n)=(3,3),(4,3)$ or $(5,5)$. But this contradicts [6, Theorem 5.4.22]. □

Proposition 6.4.4 *Suppose $n \geqslant 4-u$ and $(n,q) \neq (6/u,2)$ and let G be a subgroup of X. Suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is either $\mathrm{PSU}_k(s)$, $\mathrm{P\Omega}_{2k}^-(s)$ or ${}^2\mathrm{E}_6(s)$, where $s = p^b$. Then G does not contain a linear Singer cycle of X.*

Proof. By [24, Proposition 5.4.6], we either have $b = af$ or $2b = af$ and a does not divide b, for some positive integer f. Suppose first that $b = af$. Then Inequality 6.4.4 holds. If $S = {}^2\mathrm{E}_6(s)$, then this inequality becomes

$$18f \geqslant un \geqslant 27^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$ then we get $18f \geqslant 27^f$, which cannot happen. So $X \neq \mathrm{GU}_{2n}(q)$ and so $18^f \geqslant 27^f/2$, which gives $f = 1$. Hence n divides 18 and since $n \geqslant 27/2$ we have $2n = 36$. But by [26], this cannot happen.

If $S = \mathrm{P\Omega}_{2k}^-(s)$, then Inequality 6.4.4 becomes

$$2kf \geqslant un \geqslant (2k)^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we get $2kf \geqslant (2k)^f$. Thus $f = 1$, $n = k$ and we have an embedding of $\mathrm{P\Omega}_{2n}^-(q)$ in $\mathrm{PGU}_{2n}(q)$. By Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}\left(\mathrm{P\Omega}_{2n}^-(q)\right)$ is $q^{n+1}/(q-1)$. But if G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, then we have

$$\left(q^{2n}-1\right)/(q+1) \leqslant q^{n+1}/(q-1),$$

which has no integer solutions for $n \geqslant 4$ and q a power of a prime.

Hence $X \neq \mathrm{GU}_{2n}(q)$ and we have $2kf \geqslant (2k)^f/2$. Thus $f = 1$, so n divides $2k$ and since $n \geqslant k$, we either have $n = 2k$ or $n = k$. If $n = 2k$, then we have a possible embedding of $\mathrm{P\Omega}_n^-(q)$ in $\mathrm{PSp}_{2n}(q)$ or $\mathrm{PGO}_{2n}^+(q)$. By Theorem 2.2.6, an upper bound on the element order of $\mathrm{Aut}\left(\mathrm{P\Omega}_n^-(q)\right)$ is $q^{(n+2)/2}/(q-1)$, so since G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$, then we have

$$(q^n-1)/\gcd(2,q-1) \leqslant q^{(n+2)/2}/(q-1),$$

which has no integer solutions for $n \geqslant 8$ and q a power of a prime.

So $n = k \geqslant 4$ and we have a possible embedding of $\mathrm{P}\Omega^-_{2n}(q)$ in $\mathrm{PSp}_{2n}(q)$ or $\mathrm{PGO}^+_{2n}(q)$. If $X = \mathrm{GO}^+_{2n}(q)$, then the order of $\mathrm{P}\Omega^-_{2n}(q)$ is divisible by a primitive prime divisor of $q^{2n}-1$, but the order of $\mathrm{PGO}^+_{2n}(q)$ is not. Hence $\mathrm{P}\Omega^-_{2n}(q)$ cannot embed in $\mathrm{PGO}^+_{2n}(q)$.

If $X = \mathrm{Sp}_{2n}(q)$, then by [6, Lemma 1.12.4], $\mathrm{P}\Omega^-_{2n}(q)$ does not embed in $\mathrm{PSp}_{2n}(q)$, if q is odd. Also, if q is even, then $\mathrm{P}\Omega^-_{2n}(q)$ in contained in a member of $\mathcal{C}_8$.

If $S = \mathrm{PSU}_k(s)$, then combining Inequality 6.4.4 and [24, Proposition 5.4.8], we get

$$2kf \geqslant un \geqslant \begin{cases} k^f(k-1)^f u/2, & k \geqslant 7, \\ 20^f u/2, & 5 \leqslant k \leqslant 6, \\ 6^f u/2, & 3 \leqslant k \leqslant 4. \end{cases}$$

If $X = \mathrm{GU}_{2n}(q)$, then this gives $f = 1$ and $k = 3$ or 4. If $k = 4$, then $2n$ divides 8. Since $2n \geqslant 6$, we have $2n = 8$. But by [26], this cannot happen.

So $k = 3$, then $2n = 6$ and we have a possible embedding of $\mathrm{PSU}_3(q)$ in $\mathrm{PGU}_6(q)$. If G contains a linear Singer cycle of $\mathrm{GU}_6(q)$, then using the element order bounds in Theorem 2.2.6, Inequality 6.1.1 gives

$$\left(q^6-1\right)/(q+1) \leqslant \begin{cases} q^2+1, & q > p,\ q \neq 4, \\ 16, & q = 4, \\ (q+1)q, & q = p, \end{cases}$$

which has no solutions for q a power of a prime.

Therefore $X \neq \mathrm{PGU}_{2n}(q)$ and from the above bounds on n, we have $f = 1$ and

$3 \leqslant k \leqslant 6$. If $k = 6$, then n divides 12. Since $n \geqslant 10$, we have $2n = 24$. But this contradicts [26]. Similarly, if $k = 5$, then $2n = 20$ contradicting [26]. If $k = 4$, then n divides 8 and so since $n \geqslant 3$, we either have $2n = 16$ or $2n = 8$. The latter case is ruled out by [26], whereas if $2n = 16$, then the order of $\mathrm{PSU}_4(q)$ is not divisible by a primitive prime divisor of $q^n - 1$. Hence $k = 3$. In this case n divides 6, so since $n \geqslant 3$, either $2n = 12$ or $2n = 6$. But the former is ruled out by [26] and if $2n = 6$, then the order of $\mathrm{PSU}_3(q)$ is not divisible by a primitive prime divisor of $q^n - 1$.

Therefore we can assume $2b = af$, where a does not divide b. Then Inequality 6.4.5 holds. If $S = {}^2\mathrm{E}_6(s)$, then this becomes

$$9f \geqslant un \geqslant 27^f u/2,$$

which is impossible.

If $S = \mathrm{P}\Omega_{2k}^{-}(s)$, then Inequality 6.4.5 becomes

$$kf \geqslant un \geqslant (2k)^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we have $kf \geqslant (2k)^f$, which cannot happen. So $X \neq \mathrm{GU}_{2n}(q)$ and $kf \geqslant (2k)^f/2$, which gives $f = 1$ and $n = k$. We therefore have a possible embedding of $\mathrm{P}\Omega_{2n}^{-}(s)$ in $\mathrm{PSp}_{2n}(s^2)$ or $\mathrm{PGO}_{2n}^{+}(s^2)$. If G contains a linear Singer cycle of X, then using the element order bounds in Theorem 2.2.6, we have

$$\left(\left(s^2\right)^n - 1\right) / \gcd\left(2, s^2 - 1\right) \leqslant s^{n+1} / (s-1),$$

which has no integer solutions for $n \geqslant 4$ and s a power of a prime.

Finally, if $S = \mathrm{PSU}_k(s)$, then Inequality 6.4.5 gives

$$kf \geqslant un \geqslant k^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we get $kf \geqslant k^f$ and so $f = 1$ and $2n = k$. But then the order of $\mathrm{PSU}_{2n}(s)$ is not divisible by a primitive prime divisor of $(s^2)^{2n} - 1$.

So $X \neq \mathrm{GU}_{2n}(q)$ and we have $kf \geqslant k^f/2$. By our assumptions on a and b, we get $f = 1$. Now $2n \leqslant 2k \leqslant k(k+1)/2$, so by [24, Proposition 5.4.11], either $2n = k$ or $(k, n) = (3,3), (4,3), (5,5)$. By [6, Theorem 5.4.22], these latter three cases do not occur, so we have a possible embedding of $\mathrm{PSU}_{2n}(s)$ in $\mathrm{PSp}_{2n}(s^2)$ or $\mathrm{PGO}^+_{2n}(s^2)$. If G contains a linear Singer cycle of X, then using the bounds in Theorem 2.2.6, we have

$$\left((s^2)^n - 1\right) / \gcd\left(2, s^2 - 1\right) \leqslant \begin{cases} s^{2n-1} + 1, & s > 2, \\ 4\left(2^{2n-3} + 1\right), & s = 2, \end{cases}$$

which has no integer solutions for $n \geqslant 3$ and s a power of a prime. □

Proposition 6.4.5 *Suppose $n \geqslant 4 - u$ and $(n, q) \neq (6/u, 2)$ and let G be a subgroup of X. Suppose that G lies in $\mathcal{S}$ and the socle of $G/\mathrm{Z}(X)$ is ${}^3\mathrm{D}_4(s)$, where $s = p^b$. Then G does not contain a linear Singer cycle of X.*

Proof. By [24, Remark 5.4.7], we either have $b = af$ or $3b = af$ and a does not divide b, for some positive integer f. Suppose $b = af$. Then Inequality 6.4.4 holds, so using Table 6.6, we have

$$12f \geqslant un \geqslant 8^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, then we get $12f \geqslant 8^f$ and so $f = 1$. This means $2n$ divides 12. Since we also have $2n \geqslant 8$, this means $2n = 12$. But by [26], ${}^3\mathrm{D}_4(s)$ has no irreducible 12-degree representations.

So $X \neq \mathrm{GU}_{2n}(q)$ and we have $12f \geqslant 8^f/2$. Hence $f = 1$. This time n divides 12 and $n \geqslant 4$ and so $2n = 8$, 12 or 24. Using [26], we only need to consider $2n = 8$. Hence we have a possible embedding of ${}^3\mathrm{D}_4(q)$ in $\mathrm{PGO}_8^+(q)$ or $\mathrm{PSp}_8(q)$. Let r be a primitive prime divisor of $q^4 - 1$. If G contains a linear Singer cycle of X, then by our assumptions, r divides the order of ${}^3\mathrm{D}_4(s)$, and so by inspection, we see that r divides $q^8 + q^4 + 1$. This means r divides

$$q^8 + q^4 + 1 - \left(q^4 + 2\right)\left(q^4 - 1\right) = 3,$$

so $r = 3$. But by Remarks 2.2.3, $r \geqslant n + 1 = 5$, a contradiction.

Therefore we can assume $3b = af$ and a does not divide b. Then Inequality 6.4.5 holds, so by Table 6.6, we have

$$4n \geqslant un \geqslant 8^f u/2.$$

If $X = \mathrm{GU}_{2n}(q)$, we get $4f \geqslant 8^f$, which cannot happen. So $X \neq \mathrm{GU}_{2n}(q)$ and $4f \geqslant 8^f/2$, which means $f = 1$ and $n = 4$. We therefore have a possible embedding of ${}^3\mathrm{D}_4(s)$ in either $\mathrm{PGO}_8^+(s^3)$ or $\mathrm{PSp}_8(s^3)$.

Now, by [28, Table 2], an upper bound for the element order of $\mathrm{Aut}\left({}^3\mathrm{D}_4(s)\right)$ is

$$7p\,(s+1)^2 \cdot 3b \leqslant 21s\,(s+1)^2.$$

Since G contains a linear Singer cycle of X, we have

$$\left(\left(s^3\right)^4 - 1\right)/\gcd\left(2, s^3 - 1\right) \leqslant 21s\,(s+1)^2,$$

which has no solutions for s a power of a prime. □

This concludes the defining characteristic case and the proof of the main theorems.

Chapter 7

Concluding remarks

In this thesis, we have proved the following results.

Theorem 7.0.1 *Let $G \leqslant \mathrm{Sp}_{2n}(q)$ with $n \geqslant 4$ and suppose that G contains a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$. Then G is contained in one of the following:*

1. $\mathrm{Stab}_{\mathrm{Sp}_{2n}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{Sp}_{2n}(q)}(W_2)$. *Both groups have the structure* $q^{n(n+1)/2} : \mathrm{GL}_n(q)$*;*
2. $\mathrm{GL}_n(q).2$*, with q odd;*
3. $\mathrm{Sp}_{2n/s}(q^s).s$*, where s is a prime dividing n;*
4. $\mathrm{GU}_n(q).2$*, with n even and q odd; or*
5. $\mathrm{GO}^+_{2n}(q)$*, with q even.*

Theorem 7.0.2 *Let $G \leqslant \mathrm{GU}_{2n}(q)$ with $n \geqslant 3$ and suppose that G contains a linear Singer cycle of $\mathrm{GU}_{2n}(q)$. Then G is contained in one of the following:*

1. $\mathrm{Stab}_{\mathrm{GU}_{2n}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{GU}_{2n}(q)}(W_2)$. *Both groups have the structure* $q^{n^2} : \mathrm{GL}_n(q^2)$*;*
2. $\mathrm{GL}_n(q^2).2$*; or*
3. $\mathrm{GU}_{2n/s}(q^s).s$*, where s is an odd prime.*

Theorem 7.0.3 *Let $n \geqslant 5$ and let G be a subgroup of $\mathrm{GO}_{2n}^{+}(q)$ not containing $\Omega_{2n}^{+}(q)$ and suppose that G contains a linear Singer cycle of $\mathrm{GO}_{2n}^{+}(q)$. Then G is contained in one of the following:*

1. $\mathrm{Stab}_{\mathrm{GO}_{2n}^{+}(q)}(W_1)$ *or* $\mathrm{Stab}_{\mathrm{GO}_{2n}^{+}(q)}(W_2)$. *Both groups have the structure* $q^{n(n-1)/2} : \mathrm{GL}_n(q)$;
2. $\mathrm{GL}_n(q).2$;
3. $\mathrm{GO}_{2n/s}^{+}(q^s).s$, *where s is a prime dividing n; or*
4. $\mathrm{GU}_n(q).2$ *with n even.*

As a consequence of these, we obtain the following corollary.

Corollary 7.0.4 *Let X be one of* $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_{2n}(q)$ *or* $\mathrm{GO}_{2n}^{+}(q)$, *where*

$$n \geqslant \begin{cases} 4, & \text{if } X = \mathrm{Sp}_{2n}(q), \\ 3, & \text{if } X = \mathrm{GU}_{2n}(q), \\ 5, & \text{if } X = \mathrm{GO}_{2n}^{+}(q). \end{cases}$$

Also, let G be an irreducible subgroup of X that does not contain $\Omega_{2n}^{+}(q)$ when $X = \mathrm{GO}_{2n}^{+}(q)$. If G contains a linear Singer cycle of X, then one of the following holds:

1. *G is contained in* $\mathrm{GL}_n(q^u).2$;
2. $X = \mathrm{Sp}_{2n}(q)$ *and G is contained in* $\mathrm{Sp}_{2n/s}(q^s).s$, *where s is a prime dividing n;*
3. $X = \mathrm{GU}_{2n}(q)$ *and G is contained in* $\mathrm{GU}_{2n/s}(q^s).s$, *where s is an odd prime;*
4. $X = \mathrm{GO}_{2n}^{+}(q)$ *and G is contained in* $\mathrm{GO}_{2n/s}^{+}(q^s).s$, *where s is a prime dividing n;*
5. *n is even, $X = \mathrm{Sp}_{2n}(q)$ with q odd, or $X = \mathrm{GO}_{2n}^{+}(q)$ and G is contained in* $\mathrm{GU}_n(q).2$; *or*

6. $X = \mathrm{Sp}_{2n}(q)$ *with* q *even and* G *is contained in* $\mathrm{GO}^+_{2n}(q)$.

This corollary, together with Theorem 2.1.4 allows us to inductively determine all irreducible subgroups containing linear Singer cycles.

For example, if G is an irreducible subgroup of $\mathrm{Sp}_{2n}(q)$ containing a linear Singer cycle of $\mathrm{Sp}_{2n}(q)$, then by Corollary 7.0.4, G lies in $\mathrm{GL}_n(q).2$, $\mathrm{Sp}_{2n/s}(q^s).s$, $\mathrm{GU}_n(q).2$ or $\mathrm{GO}^+_{2n}(q)$. If G is contained in $\mathrm{GL}_n(q).2$, then we can use Theorem 2.1.4 to determine the possibilities for G. If G lies in $\mathrm{Sp}_{2n/s}(q^s).s$, then we use the subgroup list for the symplectic groups in Corollary 7.0.4 again and repeat the argument. If G lies in $\mathrm{GU}_n(q).2$, then we use the subgroup list for the unitary groups in Corollary 7.0.4 and repeat the argument. If G lies in $\mathrm{GO}^+_{2n}(q)$, we use the subgroups list for the orthogonal groups in Corollary 7.0.4 and again repeat the argument. We can do this in a similar way when $X = \mathrm{GU}_{2n}(q)$ or $\mathrm{GO}^+_{2n}(q)$.

For small values of n, the method is similar. However G could lie in one of the exceptional cases to the main theorems and the small dimensional cases. If this occurs, then the possibilities for G can be determined using MAGMA.

Our results complement Theorem 2.1.7, since we look at the plus type orthogonal groups and the even-dimensional unitary groups which are not dealt with in Bereczky's result. We imagine our results could have similar applications as Bereczky's and Kantor's results. These applications include Abhyankar and Keskar [1, Theorem 1.9], where Kantor's Theorem is used to determine the structure of a Galois group and Fairbairn et al [12], where B ereczky's Theorem is used for results on Beauville groups.

We imagine our results could be applied to any situation involving a group containing a linear Singer cycle.

Appendix A

Computer programs

At certain points in this thesis, we use MAGMA [5] to determine if specific subgroups in either $\mathrm{GO}_8^+(2)$ or $\mathrm{Sp}_8(2)$ contain a linear Singer cycle. We provide the necessary details here.

A.1 The tensor product stabilizer in $\mathrm{GO}_8^+(2)$

The following process shows that the tensor product stabilizer, $\mathrm{Sp}_4(2) \circ \mathrm{Sp}_2(2)$ in $\mathrm{GO}_8^+(2)$ contains a linear Singer cycle. This is needed in the proof of Proposition 5.4.4.

```
> G:=GeneralOrthogonalGroupPlus(8,2);

> X:=Subgroups(G:OrderEqual:=15);

> #X;

2

> for i in [1..2] do #Centraliser(G,X[i]‘subgroup); end for;

30

15
```

This shows that up to conjugacy, there are two conjugacy classes of subgroups of order 15, only one of which is self-centralizing. This one is conjugate to the linear Singer subgroup by Corollary 3.3.2.

```
> S:=Subgroups(G:OrderEqual:=4320);
> #S;
8
> for i in [1..8] do IsTensor(S[i]`subgroup); end for;
false
false
false
false
false
false
false
true
> S8:=S[8]`subgroup;
> TensorFactors(S8);
   MatrixGroup(4, GF(2))
    Generators:
        [1 1 0 1]
        [0 1 1 1]
        [1 1 1 0]
        [0 0 1 0]


        [0 1 1 0]
        [0 1 0 0]
        [1 1 1 1]
        [0 1 0 1]
```

```
        [0 1 0 0]
        [1 1 0 0]
        [1 1 1 1]
        [1 0 1 0],
    MatrixGroup(2, GF(2))
    Generators:
        [1 1]
        [1 0]


        [1 1]
        [0 1]
```

This finds the tensor product stabilizer.

```
> Y:=Subgroups(S8:OrderEqual:=15);
> #Y;
1
> #Centraliser(G,Y[1]`subgroup);
15
```

Finally, this shows that the subgroup of order 15 is the tensor product stabilizer is self-centralizing and so is conjugate to the linear Singer subgroup.

A.2 The subgroups of $\mathrm{GO}_8^+(2)$ isomorphic to A_9

This process shows that of the two subgroups of $\mathrm{GO}_8^+(2)$ isomorphic to A_9, one contains the linear Singer cycle, the other does not. This also shows that the subgroup of $\mathrm{GO}_8^+(2)$ isomorphic to S_9 does not contains a linear Singer cycle. We use these arguments in Theorem 6.2.2.

```
> G:=GeneralOrthogonalGroupPlus(8,2);
> S:=Subgroups(G:OrderEqual:=181440);
> #S;
2
> S1:=S[1]`subgroup;
> S2:=S[2]`subgroup;
> Isom1:=IsIsomorphic(S1,Alt(9));
> Isom1;
true
> Isom2:=IsIsomorphic(S2,Alt(9));
> Isom2;
true
```

This argument finds both subgroups isomorphic to A_9 in $GO_8^+(2)$, up to conjugacy.

```
> X:=Subgroups(S1:OrderEqual:=15);
> #X;
1
> #Centraliser(G,X[1]`subgroup);
30
```

This shows that the subgroup of order 15 in one copy of A_9 is not self-centralizing and cannot be conjugate to the linear Singer subgroup.

```
> Y:=Subgroups(S2:OrderEqual:=15);
> #Y;
1
> #Centraliser(G,Y[1]`subgroup);
15
```

This shows that the subgroup of order 15 in the other copy of A_9 is self-centralizing and so is conjugate to the linear Singer subgroup.

```
> T:=Subgroups(G:OrderEqual:=362880);
> #T;
1
> T1:=T[1]‘subgroup;
> Isom3:=IsIsomorphic(T1,Sym(9));
> Isom3;
true
> Z:=Subgroups(T1:OrderEqual:=15);
> #Z;
1
> #Centraliser(G,Z[1]‘subgroup);
30
```

Finally, this argument finds the subgroup of $GO_8^+(2)$ isomorphic to S_9, up to conjugacy and shows that the subgroup of order 15 lying inside it is not self-centralizing and so cannot be conjugate to the linear Singer subgroup.

A.3 The subgroups of $Sp_8(2)$ isomorphic to S_{10}

This process shows that the subgroup of $Sp_8(2)$ isomorphic to S_{10} does not contain a linear Singer cycle. This argument is also used in the proof of Theorem 6.2.2.

```
> G:=SymplecticGroup(8,2);
> X:=Subgroups(G:OrderEqual:=15);
> #X;
3
```

```
> for i in [1..3] do #Centraliser(G,X[i]`subgroup); end for;
90
90
15
```

This shows that up to conjugacy, there are three conjugacy classes of subgroups of order 15, only one of which is self-centralizing. By Corollary 3.3.2, this one is conjugate to the linear Singer subgroup.

```
> S:=Subgroups(G:OrderEqual:=3628800);
> #S;
1
> S1:=S[1]`subgroup;
> Isom:=IsIsomorphic(S1,Sym(10));
> Isom;
true
```

This finds the subgroup isomorphic to S_{10}, up to conjugacy.

```
> Y:=Subgroups(S1:OrderEqual:=15);
> #Y;
1
> #Centraliser(G,Y[1]`subgroup);
90
```

Finally, this shows that the subgroup of order 15 lying in S_{10} is not self-centralizing and cannot be conjugate to the linear Singer subgroup.

List of References

[1] S. S. Abhyankar and P. H. Keskar. Descent principle in modular Galois theory. *Proceedings of the Indian Academy of Sciences-Mathematical Sciences*, 111(2):139–149, 2001.

[2] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones mathematicae*, 76(3):469–514, 1984.

[3] M. Aschbacher. *Finite group theory*, volume 10. Cambridge University Press, 2000.

[4] Á. Bereczky. Maximal overgroups of Singer elements in classical groups. *Journal of Algebra*, 234(1):187–206, 2000.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[6] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups.* Cambridge University Press, 2013.

[7] J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, and A. Maróti. Sets of elements that pairwise generate a linear group. *Journal of Combinatorial Theory, Series A*, 115(3):442–465, 2008.

[8] D. Bubboloni, M.S. Lucido, and T. Weigel. 2-coverings of classical groups. *arXiv preprint arXiv:1102.0660*, 2011.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups.* Oxford University Press, Oxford, 1985.

[10] L. E. Dickson. Representations of the general symmetric group as linear groups in finite and infinite fields. *Transactions of the American Mathematical Society*, 9(2):121–148, 1908.

[11] L. E. Dickson. *Linear groups with an exposition of Galois field theory.* Courier Dover Publications, 2003.

[12] B. Fairbairn, K. Magaard, and C. Parker. Generation of finite quasisimple groups with an application to groups acting on Beauville surfaces. *Proceedings of the London Mathematical Society*, 107(4):744–798, 2013.

[13] W. Feit. On large Zsigmondy primes. *Proceedings of the American Mathematical Society*, 102(1):29–36, 1988.

[14] S. Guest, J. Morris, C. Praeger, and P. Spiga. On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *arXiv preprint arXiv:1301.5166*, 2013.

[15] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl. Linear groups with orders having certain large prime divisors. *Proceedings of the London Mathematical Society*, 78(1):167–214, 1999.

[16] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II. *Journal of Algebra*, 93(1):151–164, 1985.

[17] Gerhard Hiss and Gunter Malle. Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math*, 4:22–63, 2001.

[18] B. Huppert. *Endliche Gruppen*, volume 1. Springer Berlin-Heidelberg-New York, 1967.

[19] B. Huppert. Singer-Zyklen in Klassischen Gruppen. *Mathematische Zeitschrift*, 117(1):141–150, 1970.

[20] C. Jansen. The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comput. Math*, 8(122-144):62, 2005.

[21] W. M. Kantor. Linear groups containing a Singer cycle. *Journal of Algebra*, 62(1):232–234, 1980.

[22] W. M. Kantor and Á. Seress. Large element orders and the characteristic of Lie-type simple groups. *Journal of Algebra*, 322(3):802–832, 2009.

[23] O. H. King. The subgroup structure of finite classical groups in terms of geometric configurations. In *Surveys in Combinatorics*, pages 29–56, 2005.

[24] P. B. Kleidman and M. W. Liebeck. *The subgroup structure of the finite classical groups*, volume 129. Cambridge University Press, 1990.

[25] V. Landazuri and G. M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *Journal of algebra*, 32(2):418–443, 1974.

[26] F. Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS Journal of Computation and Mathematics*, 4:135–169, 2001.

[27] G. Malle, J. Saxl, and T. Weigel. Generation of classical groups. *Geometriae Dedicata*, 49(1):85–116, 1994.

[28] P. Müller. Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Siegel functions. *arXiv preprint math/0110060*, 2001.

[29] G. M. Seitz. On the subgroup structure of classical groups. *Communications in Algebra*, 10(8):875–885, 1982.

[30] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, 1938.

[31] M. Suzuki. Group theory I. *Spring-Verlag, New York*, 1982.

[32] J. Thévenaz. Maximal subgroups of direct products. *Journal of Algebra*, 198(2):352–361, 1997.

[33] A. Wagner. The faithful linear representation of least degree of S_n and A_n over a field of characteristic 2. *Mathematische Zeitschrift*, 151(2):127–137, 1976.

[34] A. Wagner. The faithful linear representations of least degree of S_n and A_n over a field of odd characteristic. *Mathematische Zeitschrift*, 154(2):103–114, 1977.

[35] A. Wagner. An observation on the degrees of projective representations of the symmetric and alternating group over an arbitrary field. *Archiv der Mathematik*, 29(1):583–589, 1977.

[36] R. Wilson. *The Finite Simple Groups*, volume 251. Springer Verlag, 2009.

[37] K Zsigmondy. Zur theorie der potenzreste. *Monatshefte für Mathematik*, 3(1):265–284, 1892.